IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	: **Shinya YAMAMURA,et al.**
Filed	: **Concurrently herewith**
For	: **PROXY NETWORK CONTROL ....**
Serial No.	: **Concurrently herewith**

November 25, 2003

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRIORITY CLAIM AND

SUBMISSION OF PRIORITY DOCUMENT

S I R:

Applicant hereby claims priority under 35 USC 119 from **Japanese** patent application number **2002-346949** filed **November 29, 2002,** a certified copy of which is enclosed.

Respectfully submitted,

Thomas J. Bean
Reg. No. 44,528

Katten Muchin Zavis Rosenman
575 Madison Avenue
New York, NY 10022-2585
(212) 940-8800
Docket No.: FUJH 20.761

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１１月２９日

出願番号
Application Number: 特願２００２－３４６９４９

[ST. 10/C]: [ＪＰ２００２－３４６９４９]

出願人
Applicant(s): 富士通株式会社

２００３年　８月　１日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０６１９１３

【書類名】　特許願

【整理番号】　0253396

【提出日】　平成14年11月29日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 12/24

H04L 12/66

G06F 13/00

【発明の名称】　代理ネットワーク制御装置

【請求項の数】　10

【発明者】

【住所又は居所】　福岡県福岡市早良区百道浜２丁目２番１号　富士通西日本コミュニケーション・システムズ株式会社内

【氏名】　山村　新也

【発明者】

【住所又は居所】　福岡県福岡市早良区百道浜２丁目２番１号　富士通西日本コミュニケーション・システムズ株式会社内

【氏名】　佐藤　義治

【発明者】

【住所又は居所】　福岡県福岡市早良区百道浜２丁目２番１号　富士通西日本コミュニケーション・システムズ株式会社内

【氏名】　中村　勝一

【発明者】

【住所又は居所】　福岡県福岡市早良区百道浜２丁目２番１号　富士通西日本コミュニケーション・システムズ株式会社内

【氏名】　堀口　辰雄

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100094514

【弁理士】

【氏名又は名称】　林　恒徳

【選任した代理人】

【識別番号】　100094525

【弁理士】

【氏名又は名称】　土井　健二

【手数料の表示】

【予納台帳番号】　030708

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9704944

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　代理ネットワーク制御装置

【特許請求の範囲】

【請求項１】　ユーザ端末に所定のサービスを提供するサービス装置に代行して，該サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置であって，

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視するパケット監視部と，

前記パケット監視部により監視されたパケットに基づいて前記補完または拡張する機能を決定して実行する実行部と，

を備えている代理ネットワーク制御装置。

【請求項２】　ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置を制御することにより，前記サービス装置の機能を補完または拡張する機能を前記サービス装置に代行して実行する代理ネットワーク制御装置であって，

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視するパケット監視部と，

前記パケット監視部により監視されたパケットに基づいて前記補完または拡張する機能を決定するサービス制御部と，

前記サービス制御部により決定された機能に基づいて前記ネットワーク装置を制御する外部機器制御部と，

を備えている代理ネットワーク制御装置。

【請求項３】　請求項２において，

前記サービス装置はＤＨＣＰサーバであり，

前記パケット監視部は，前記サービス装置から前記ユーザ端末に発行されるアドレスを含んだパケットを監視し，

前記サービス制御部は，前記パケット監視部により監視されたパケットに基づいて，前記サービス装置により発行されたアドレスを送信元アドレスとして有す

るパケットを通過させ，それ以外のアドレスを送信元アドレスとして有するパケットを通過させないアクセス規制機能を決定し，

前記外部機器制御部は，前記アクセス規制機能を実行するように前記ネットワーク装置を制御する，

代理ネットワーク制御装置。

【請求項４】　請求項２において，

前記ユーザ端末がホームネットワークのホームアドレスを有する移動通信端末であり，前記ネットワーク装置が前記ホームネットワークの外部ネットワークから外部に送信されるパケットのうち，所定の送信元アドレスを有するパケットを通過させ，それ以外のパケットを通過させないファイアウォールであり，

前記パケット監視部は，前記外部ネットワークに移動した前記ユーザ端末と前記ホームネットワークのホームエージェントとの間で通信される，前記ユーザ端末のホームアドレスを含んだパケットを監視し，

前記サービス制御部は，前記パケット監視部により監視されたパケットに基づいて，前記ホームアドレスを有するパケットを通過させるようにアクセス規制を解除する機能を決定し，

前記外部機器制御部は，前記アクセス規制を解除する機能を実行するように，前記ネットワーク装置を制御する，

代理ネットワーク制御装置。

【請求項５】　請求項２において，

前記ユーザ端末がＩＰｖ６端末であり，前記サービス装置が生成された前記ユーザ端末のＩＰアドレスの認証を行う認証サーバであり，

前記パケット監視部は，前記サービス装置により認証されたＩＰアドレスを含むパケットを監視し，

前記サービス制御部は，前記パケット監視部により監視されたパケットに基づいて，前記ＩＰアドレスを送信元アドレスとして有するパケットを通過させるようにアクセス規制を解除する機能を決定し，

前記外部機器制御部は，前記アクセス規制を解除する機能を実行するように，前記ネットワーク装置を制御する，

代理ネットワーク制御装置。

【請求項６】　コンピュータに，

ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間で通信されるパケットを監視する手順と，

前記監視したパケットに基づいて，前記サービス装置に代行して，該サービス装置の機能を補完または拡張する機能を決定して実行する手順と，

を実行させるためのプログラム。

【請求項７】　ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置を制御することにより，前記サービス装置の機能を補完または拡張する機能を前記サービス装置に代行して実行するコンピュータに，

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視する手順と，

前記監視したパケットに基づいて前記補完または拡張する機能を決定する手順と，

前記決定した機能に基づいて前記ネットワーク装置を制御する手順と，

を実行させるためのプログラム。

【請求項８】　ユーザ端末と通信を行い該ユーザ端末に所定のサービスを提供するサービス装置と，

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視し，所定の条件を満たすパケットに基づいて，前記サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置と，

を備えているネットワークシステム。

【請求項９】　ユーザ端末と通信を行い該ユーザ端末に所定のサービスを提供するサービス装置と，

前記ユーザ端末と前記サービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置と，

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視し，所

定の条件を満たすパケットに基づいて前記ネットワーク装置を制御することにより，前記サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置と，

を備えているネットワークシステム。

【請求項１０】　請求項９において，

前記サービス装置はＤＨＣＰサーバであり，

前記代理ネットワーク制御装置は，前記サービス装置から前記ユーザ端末に配布されるアドレスを含んだパケットを監視し，前記ユーザ端末から送信される，前記アドレスを送信元アドレスとして有するパケットを通過させ，それ以外のパケットを通過させないように前記ネットワーク装置を制御する，

ネットワークシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は，ネットワークの機能を代理実行する代理ネットワーク制御装置に関し，特に，ユーザ端末に所定のサービスを提供するサービス装置に代行して，該サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置に関する。

【０００２】

また，本発明は，ネットワークの機能を代理実行するコンピュータに実行させるためのプログラムに関し，特に，ユーザ端末に所定のサービスを提供するサービス装置に代行して，該サービス装置の機能を補完または拡張する機能をコンピュータに実行させるためのプログラムに関する。

【０００３】

さらに，本発明は，このような代理ネットワーク制御装置を有するネットワークシステムに関する。

【０００４】

【従来の技術】

インターネット（ＩＰネットワーク）の普及に伴い，どこからでも自由にＩＰ

ネットワークに接続できるような環境が整いつつある。このような環境は，ネットワークを利用するユーザにとって利便性が向上する一方で，ネットワークを管理する側にとって誰でもネットワークに接続できるので，セキュリティの観点から問題がある。

【０００５】

特に，ＤＨＣＰ（Dynamic Host Configuration Protocol）やＩＰｖ６等のプロトコルによると，アドレスが自動的に作成されユーザに発行されるので，ユーザはアクセスする場所のアドレス情報を知らなくても，ネットワークにアクセスできる。

【０００６】

したがって，今後，セキュリティの観点から，アクセス権限を有しないユーザのアクセスを制限するアクセス規制が重要となってくる。

【０００７】

アクセス規制を行うため，アクセス規制機能を有するネットワーク装置とユーザの認証を行う認証装置とを組み合わせたり，ＤＨＣＰを実行するＤＨＣＰサーバにネットワーク装置の制御機能を付加することによりアクセス規制を行う提案が行われ，製品も登場しつつある（例えば特許文献１～４参照）。

【０００８】

また，端末のネットワークへの接続を制御する方式としては，制御サーバ（認証サーバ，ＤＨＣＰサーバ等）と制御装置（ファイアウォール，パケットシェーピング装置等）とを組み合わせて，ユーザを認証後，ユーザ端末からネットワークへの接続を許容することが従来の技術で行われている。

【０００９】

ネットワークの機能を代理実行するものとしては，ＷＥＢコンテンツをキャッシュし，コンテンツのオリジナルを提供しているサーバとは別のサーバが代理でＷＥＢコンテンツをユーザに提供するプロキシサーバがある。プロキシサーバは，利用ユーザが明示的にサーバのアドレスを指定するものと，ネットワーク側で強制的にパケットを捕捉し，プロキシサーバの機能を実行する透過型プロキシとがある。

【００１０】

ネットワークの制御を，所定の指針で行う仕組みとしてはポリシーベースネットワーク（ＰＢＮ：Policy Based Network）がある。ＰＢＮは，指定されたパケットを捕捉するポリシーデテクションポイントと，捕捉したパケットに対するポリシー（動作）を決定するポリシーサーバと，決定されたポリシーに基づき該当するトラフィックの制御を行うポリシー実施ポイントとで構成される。

【００１１】

トラフィックを監視するものとしては，sniffer，etherealといったプロトコルモニタが存在する。

【００１２】

【特許文献１】

特開２００１－３２６６９６号公報

【００１３】

【特許文献２】

特開２００１－３６５６１号公報

【００１４】

【特許文献３】

特開２００１－２７４８０６号公報

【００１５】

【特許文献４】

特開平１１－２４３３８９号公報

【００１６】

【発明が解決しようとする課題】

しかし，ＤＨＣＰサーバに新たな機能を追加する場合には，これまで使用していたＤＨＣＰサーバを新たなものに変更したり，既存のＤＨＣＰサーバのプログラムやハードウェアを変更したりする必要があり，また，既存のネットワーク構成そのものを変更しなければならない場合もある。さらに，ＩＰｖ６については，提案のみがなされており，装置は存在しないのが実情である。

【００１７】

また，認証サーバと制御装置を組み合わせる方式は，認証サーバが制御装置に対して，アクセス規制を行うため，認証サーバと制御装置の組み合わせは，認証サーバの制御ソフトによって決定されてしまう。そのためアクセス規制サービスを導入しようとするネットワーク運営者は，新たな認証サーバと制御装置とをセットで購入しネットワークに組み込む必要があり，コストが高くなる。

【００１８】

プロキシサーバは，主にＨＴＴＰプロトコル専用に作られており，ＨＴＴＰ以外には，ＲＴＰ等，限られたプロトコルしかサポートしていない。また，プロキシサーバは，キャッシュされている情報をユーザからのＨＴＴＰリクエストへの応答として答えるか，コンテンツのオリジナルを格納しているサーバへ，ユーザ端末の代理として通信を行うかのいずれかの機能しか有しておらず，特定のサービスを補完するような機能を有しない。

【００１９】

また，透過型プロキシはＨＴＴＰプロトコルを強制的に横取りしているが，あくまでもプロキシサーバ内部で処理を終端しており，通常のプロキシと動作は変わらない。さらに，プロキシサーバは，アクセス規制に使用する情報がＵＲＬであり，ネットワークへのアクセス規制とは異なる機能しか実行できない。

【００２０】

ＰＢＮは，パケットを監視し，所定の指針に基づき，パケットを制御するが，パケット監視装置とポリシーサーバとをネットワークに導入しなければならない。したがって，ＰＢＮによると，ネットワークに新たな装置を導入し，またネットワークの構成の変更を伴う。

【００２１】

また，ＰＢＮでは，ポリシーを決定するための条件は，ＩＰアドレスやポート番号等のＩＰヘッダの情報に依存しており，一般にプロトコルの詳細までを解析して動作するようにはなっていない。

【００２２】

プロトコルモニタは，プロトコルを表示用に解析する機能は持っているが，解析したプロトコルを基に，何らかの動作を行う機能や，ネットワーク機器との連

携機能を具備しない。

【００２３】

本発明は，このような背景に鑑みなされたものであり，その目的は，ネットワークの既存の装置やネットワークの構成に変更を加えることなく，ネットワークの機能，特にユーザ端末にサービスを提供するサービス装置の機能を補完または拡張することができる代理ネットワーク制御装置および該代理ネットワーク制御装置を有するネットワークシステムを提供することにある。

【００２４】

【課題を解決するための手段】

前記目的を達成するために，本発明による代理ネットワーク制御装置は，ユーザ端末に所定のサービスを提供するサービス装置に代行して，該サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置であって，前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視するパケット監視部と，前記パケット監視部により監視されたパケットに基づいて前記補完または拡張する機能を決定して実行する実行部と，を備えている。

【００２５】

また，本発明による代理ネットワーク制御装置は，ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置を制御することにより，前記サービス装置の機能を補完または拡張する機能を前記サービス装置に代行して実行する代理ネットワーク制御装置であって，前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視するパケット監視部と，前記パケット監視部により監視されたパケットに基づいて前記補完または拡張する機能を決定するサービス制御部と，前記サービス制御部により決定された機能に基づいて前記ネットワーク装置を制御する外部機器制御部と，を備えている。

【００２６】

本発明によると，代理ネットワーク制御装置が，サービス装置に代わって，サービス装置の機能を補完または拡張する機能を代理実行するので，サービス装置

に機能を追加したり，サービス装置を新たなものに交換したりする必要がない。これにより，既存のネットワーク資源をそのまま使用することができ，コストを削減することができる。また，代理ネットワーク制御装置は，サービス装置とユーザ端末との間で通信されるパケットを監視できる場所であれば，どこでも設置することができる。例えばネットワーク装置が有する監視インタフェース等に代理ネットワーク制御装置を接続することができる。これにより，ネットワークの構成を変更することなく，代理ネットワーク制御装置を既存のネットワークに組み込むことができる。

【００２７】

本発明によるネットワークシステムは，ユーザ端末と通信を行い該ユーザ端末に所定のサービスを提供するサービス装置と，前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視し，所定の条件を満たすパケットに基づいて，前記サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置と，を備えている。

【００２８】

本発明によるプログラムは，コンピュータに，ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間で通信されるパケットを監視する手順と，前記監視したパケットに基づいて，前記サービス装置に代行して，該サービス装置の機能を補完または拡張する機能を決定して実行する手順と，を実行させるためのものである。

【００２９】

また，本発明によるプログラムは，ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置を制御することにより，前記サービス装置の機能を補完または拡張する機能を前記サービス装置に代行して実行するコンピュータに，前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視する手順と，前記監視したパケットに基づいて前記補完または拡張する機能を決定する手順と，前記決定した機能に基づいて前記ネットワーク装置を制御する手順と，を実行させるためのものである。

【００３０】

本発明によるプログラムによっても，上記本発明による代理ネットワーク制御装置と同様の作用効果を得ることができる。

【００３１】

本発明によるネットワークシステムは，ユーザ端末と通信を行い該ユーザ端末に所定のサービスを提供するサービス装置と，前記ユーザ端末と前記サービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置と，前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視し，所定の条件を満たすパケットに基づいて前記ネットワーク装置を制御することにより，前記サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置と，を備えている。

【００３２】

本発明によるネットワークシステムによっても，前記同様に，既存のネットワーク資源を変更することなく使用でき，また，ネットワークの構成を変更することなく，代理ネットワーク制御装置をネットワークに組み込むことができる。

【００３３】

【発明の実施の形態】

＜ネットワークシステムの構成＞

図１（Ａ）～（Ｄ）は，本発明の実施の形態による代理ネットワーク制御装置（ＰＮＣＵ：Proxy Network Control Unit）を有するネットワークシステムの構成例を示すブロック図である。

【００３４】

図１（Ａ），（Ｃ），および（Ｄ）に示すネットワークシステムは，ＰＮＣＵ１，サービスサーバ２，ユーザ端末３，およびネットワーク４に設けられた１または２以上（図１（Ａ）～（Ｄ）ではｎ個：ｎは正の整数）のネットワーク機器４１～４ｎを有する。また，図１（Ｂ）に示すネットワークシステムは，これらの構成要素に加えてハブ５をさらに有する。

【００３５】

ネットワーク４は，例えばＩＰネットワークであり，ＩＰパケットを転送する

ためのネットワーク機器４１～４ｎにより構成される。ネットワーク機器４１～４ｎは，パケットを転送する装置であり，例えばルータ，ハブ，Ｌ３スイッチ（レイヤ３スイッチ），ファイアウォール，ゲートウェイサーバ，ＮＡＴ（Network Address Translation）サーバ，ＮＡＰＴ（Network Address Port Translation）サーバ，プロキシサーバ等を含む。

【００３６】

ユーザ端末３は，ネットワーク４を介してサービスサーバ２と通信を行い，サービスサーバ２からサービスの提供を受ける端末である。ユーザ端末３として，例えばデスクトップＰＣ，ノートＰＣ，ＰＤＡ（Personal Digital Assistant）等がある。

【００３７】

サービスサーバ２は，ユーザ端末３からの要求に応じて，様々なサービスをユーザ端末３に提供するサーバである。サービスサーバ２として，例えば情報を提供するＷＥＢサーバに加えて，ネットワークアクセスやネットワーク制御等を行うＤＨＣＰサーバ，認証サーバ，ポリシーサーバ等がある。

【００３８】

ユーザ端末３とサービスサーバ２との間では，サービス用プロトコルにより通信が行われ，ユーザ端末３はサービスサーバ２よりサービスを受けることができる。サービス用プログラムとして，例えば自動ＩＰアドレス割付けサービスのためのＤＨＣＰ（Dynamic Host Configuration Protocol）や，認証サービスのための認証プロトコル等がある。

【００３９】

ＰＮＣＵ１は，ネットワーク機器４１～４ｎの一部または全てを制御して，既存のネットワークにある装置（例えばサービスサーバ２，ネットワーク機器４１～４ｎ，ハブ５，ユーザ端末３等）や構成を変更することなく，既存のネットワークにない機能を補うための装置（またはプログラム）である。既存のネットワークに補う機能としては，ネットワークセキュリティの確保（例えばネットワークに登録されていない者のネットワークへのアクセスの排除等），モバイルＩＰにおけるファイアウォールのパケットの通信確保（ファイアウォールの穴あけ）

等がある。

【００４０】

ＰＮＣＵ１は，既存のネットワークにある装置や構成を変更することなく，既存のネットワークにない機能を補完するので，ネットワークの構成要素の変更や構成の変更に伴うコストを削減することができる。ＰＮＣＵ１の詳細な構成については後に詳述する。

【００４１】

ネットワーク機器４１～４ｎを制御するために，ＰＮＣＵ１とネットワーク機器４１～４ｎとの間では，機器制御用プロトコルによる通信が行われる。この機器制御用プロトコルとして，例えば，Telnetによるコマンドラインインタフェース，ＳＮＭＰ（Simple Network Management Protocol）等がある。

【００４２】

ＰＮＣＵ１は，機能補完を行うためには，ユーザ端末３とサービスサーバ２との間で通信されるパケットを監視する。このようなＰＮＣＵ１による全パケットの監視は，図１（Ａ）～（Ｄ）のいずれの構成によっても行うことができる。

【００４３】

すなわち，図１（Ａ）に示す構成例１では，ＰＮＣＵ１がユーザ端末３とサービスサーバ２との間の通信経路上に挿入され，ユーザ端末３とサービスサーバ１との間のすべてのトラフィック（メッセージ，パケット）がＰＮＣＵ１を経由して通信される。したがって，ＰＮＣＵ１は，ユーザ端末３とサービスサーバ２との間で通信される全てのパケットを監視することができる。

【００４４】

図１（Ｂ）に示す構成例２では，ネットワーク機器４ｎとサービスサーバ２との間に，複数のユーザ端末またはサーバを集線するネットワーク装置であるハブ５が設けられ，ＰＮＣＵ１はサービスサーバ２が接続されたハブ５に接続される。この構成では，ハブ５からサービスサーバ２又はユーザ端末３に送信されるパケットが，ハブ５に接続された全ての装置に伝送レイヤ（ＯＳＩ階層モデルのレイヤ２）でブロードキャストされる。したがって，ＰＮＣＵ１は，ユーザ端末３とサービスサーバ２との間で通信されるパケットを受信し，監視することができ

る。なお，ハブ５は，ユーザ端末３とネットワーク機器４１との間に設けられてもよい。

【００４５】

図１（Ｃ）に示す構成例３では，ＰＮＣＵ１がユーザ端末３とサービスサーバ２との間の通信経路に存在するいずれかのネットワーク機器（図１（Ｃ）ではネットワーク機器４ｎ）の監視インタフェースに接続される。ネットワーク機器の監視インタフェースは，パケットを監視するためのインタフェースであり，ネットワーク機器を経由する全てのパケットが監視インタフェースから出力される。したがって，この構成でも，ＰＮＣＵ１はユーザ端末３とサービスサーバ２との間で通信されるパケットを監視することができる。

【００４６】

図１（Ｄ）に示す構成例４では，ＰＮＣＵ１がサービスサーバ２に組み込まれる。例えばＰＮＣＵ１はプログラムにより実現され，サービスサーバ２上で起動される。この構成によっても，ＰＮＣＵ１は，サービスサーバ２とユーザ端末３との間で通信されるパケットを監視することができる。

【００４７】

＜ＰＮＣＵの構成＞

図２は，ＰＮＣＵ１の機能ブロック図である。ＰＮＣＵ１は，アドレスリスト１１，サービス管理テーブル１４，アクセスリスト１１１，初期設定処理部１２，パケット監視部１３，サービス制御部１６，ロギング機能部１７，通知メッセージ制御部１８，周期処理部１９，外部機器制御部１１０，プロトコルライブラリ１５，およびコマンドラインインタフェース（ＣＬＩ：Command Line Interface）ライブラリ１１２を有する。

【００４８】

各機能ブロックはプログラムにより構成することもできるし，ハードウェア回路により構成することもできる。各機能ブロックがプログラムにより構成された場合には，このプログラムは，ＰＮＣＵ１の起動時にＰＮＣＵ１の不揮発性メモリ（ハードディスク等）から半導体メモリ（ＲＡＭ等）に呼び込まれ，ＰＮＣＵ１のＣＰＵにより実行される。

【００４９】

アドレスリスト１１は，ＰＮＣＵ１の起動時に，初期設定動作の対象を決定するために参照されるデータであり，例えば不揮発性メモリ（ハードディスク等）に記憶される。

【００５０】

図３は，アドレスリスト１１の構成例を示している。アドレスリスト１１は複数のエントリを有する。各エントリは，ＰＮＣＵ１が提供するサービス（ネットワークに補完する機能）の種別を示すサービスタイプと，複数のサービス固有情報とを有する。各サービス固有情報は，例えばアクセス規制を行う対象となるユーザ端末のＩＰアドレスである。

【００５１】

サービス管理テーブル１４は，サービスタイプ毎の処理決定テーブルへのポインタをエントリとして持つトランザクションであり，例えば揮発性メモリ（ＲＡＭ等）に記憶され，その内容はＰＮＣＵ１の動作によって動的に変更される。

【００５２】

図４は，サービス管理テーブル１４の構成例を示している。サービス管理テーブル１４は，サービスタイプで索引される処理決定テーブルへのポインタをエントリとして有し，各ポインタは，イベント名および処理実体（例えばプログラム）へのポインタを有する。

【００５３】

アクセスリスト１１１は，外部機器制御部１１０が外部機器（制御対象となっているネットワーク機器等）の制御を管理するためのトランザクションであり，例えば揮発性メモリ（ＲＡＭ等）に記憶され，その内容はＰＮＣＵ１の動作によって動的に変更される。

【００５４】

図５は，アクセスリスト１１１の構成例を示している。アクセスリスト１１１は，外部機器への設定対象となったユーザ端末のＩＰアドレス毎にエントリを有する。各エントリは，ユーザ端末のＩＰアドレス，外部機器への設定情報，状態，外部機器アドレス，およびエントリの有効時間であるタイマを有する。

【００５５】

プロトコルライブラリ１５は，サービスを提供するために解析が必要なプロトコルのメッセージの型定義とメッセージ解析プログラムにより構成される。プロトコルライブラリ１５は，サービス管理テーブル１４から参照されるイベント毎の処理実体から参照される。

【００５６】

ＣＬＩライブラリ１１２は，ネットワーク機器４１～４ｎに送出するコマンドを定義するキャラクタで構成されるコマンドライン定義文と，コマンドライン定義文に可変パラメータを埋め込んでコマンドラインを編集するコマンドライン編集プログラムと，コマンドを送り込むための通信ライブラリ（例えばTelnet）とを有する。コマンドライン定義文や通信ライブラリは，ネットワーク機器毎に異なるものを持つことができる。

【００５７】

初期設定処理部１２，ＰＮＣＵ１の起動時に最初に起動されるプログラムであり，提供するサービス機能に応じた初期設定動作を行う。初期設定動作の一例として，アクセス規制サービスを提供する場合にサービス提供対象となるユーザ端末に対するネットワーク機器へのアクセス規制フィルタの設定等がある。

【００５８】

図６は，初期設定処理部１２の処理の流れを示すフローチャートである。

【００５９】

まず，初期設定処理部１２は，アドレスリスト１１（図３参照）のエントリを１つ読み込む（Ｓ１）。続いて，初期設定処理部１２は，読み込んだエントリ内のサービスタイプにより索引されるサービス制御テーブル１４（図４参照）の処理決定テーブルへのポインタを読み込む（Ｓ２）。

【００６０】

続いて，初期設定処理部１２は，処理決定テーブルをイベント（初期設定）で索引し，該当エントリのポインタが示す処理実体（たとえばプログラム）を実行する（Ｓ３）。処理実体の処理はサービス毎に異なる。処理実体の代表的な動作としては，外部機器制御部１１０を介したネットワーク機器４１～４ｎに対する

アクセス規制フィルタの設定，パケット監視部１３へのパケット監視条件設定等が挙げられる。

【００６１】

処理実体の処理の実行完了後，初期設定処理部１２は，アドレスリスト１１の全てのエントリの読み込みが完了したかどうかを判断し（Ｓ４），完了していない場合には，再びステップＳ１～Ｓ３の処理を実行し，完了している場合には，パケット監視部１３を起動した後（Ｓ５），周期処理部１９を起動して（Ｓ６），処理を終了する。

【００６２】

パケット監視部１３は，初期設定処理部１２により起動され，初期設定処理部１２の初期化動作で設定された条件に従ってパケットの監視を行う。図７は，パケット監視部１３の処理の流れを示すフローチャートである。

【００６３】

パケット監視部１３は，パケット受信待ち状態にあり，受信されるパケットを監視する（Ｓ１１，Ｓ１２）。そして，パケット監視部１３は，パケットを受信すると（Ｓ１２でＹＥＳ），受信パケットが初期設定処理部１２により設定されたパケット捕捉条件に一致するかどうかを判断する（Ｓ１３）。

【００６４】

受信パケットがパケット捕捉条件に一致する場合には（Ｓ１３で一致），サービス制御部１６に受信パケットを与え，サービス制御部１６を起動する（Ｓ１４）。一方，受信パケットがパケット捕捉条件に一致しない場合には（Ｓ１３で不一致），パケット監視部１３は再びパケット受信待ち状態に戻る（Ｓ１１，Ｓ１２）。

【００６５】

サービス制御部１６は，パケット監視部１３により起動され，パケット監視部１３から通知されたパケット情報に基づき必要なサービス制御を行う。図８は，サービス制御部１６の処理フローを示すフローチャートである。

【００６６】

サービス制御部１６は，パケット監視部１３から通知された受信パケットの受

信ポート番号に基づいてサービスタイプを決定する（Ｓ２１）。ＩＰプロトコルでは，通信プロトコル（ＴＣＰ／ＵＤＰ等）の受信ポート番号によりサービスを識別することができるので，受信ポート番号に基づいて，サービスタイプが決定される。

【００６７】

続いて，サービス制御部１６は，受信パケットを，プロトコルライブラリ１５を参照して受信パケットのペイロード部に設定されているサービス固有プロトコルを解析し，解析した情報のうちメッセージタイプ（一般にはRequestやReply）に基づいてイベントを決定する。そして，サービス制御部１６は，決定されたサービスタイプとイベントによりサービス管理テーブル１４を索引する（Ｓ２２）。

【００６８】

続いて，サービス制御部１６は，サービス制御データにより索引したエントリが示す処理実体に従い処理を実行する（Ｓ２３）。処理実体は，例えば，サービスとイベント毎に処理コードが記述されているプログラムであり，サービスとイベントの組み合わせによって処理が異なる。なお，後述の適用例では，いくつかのサービス例を示す。

【００６９】

次に，サービス制御部１６は，処理実体の処理において，情報をロギングする場合には，ロギング機能部１７を起動し，ロギング機能部１７にロギング処理を行わせる（Ｓ２４）。

【００７０】

また，サービス制御部１６は，処理実体の処理において，他のネットワーク機器，サーバへの情報通知，プロトコル交換等が必要な場合には，通知メッセージ制御部１８を起動し，通知メッセージ制御部１８にこれらの処理を実行させる（Ｓ２５）。

【００７１】

さらに，サービス制御部１６は，処理実体の処理において，ネットワーク機器４１～４ｎ（のいずれか）に対して，パケットフィルタの設定等の制御が必要な

場合には，外部機器制御部１１０を起動し，外部機器制御部１１０に該処理を実行させる。

【００７２】

ロギング機能部１７は，ＰＮＣＵ１の提供サービスの幅を広げるための付加機能であり，捕捉したパケットの様々の情報の中から任意の情報を抽出して，ログメッセージとして編集する機能を有する。ロギング情報編集においては，編集ロジックを容易に組み込むことができるため，通常のプロトコルモニタに比較して特定のサービスに特化したきめ細かなサービスが可能になる。なお，処理の詳細はサービス毎に異なる。

【００７３】

通知メッセージ制御部１８も，ＰＮＣＵ１の提供サービスの幅を広げるための付加機能であり，捕捉したパケットの特定の情報を他のサービスサーバやネットワーク機器に通知したり，情報の交換を行うための機能を有する。処理の詳細はサービス毎に異なる。

【００７４】

ロギング機能部１７および通知メッセージ制御部１８は，サービス制御データ１４から参照される処理実体の処理を容易にするための付加機能であり，これらの機能部以外にも，処理実体間の共通の機能を切り出して新たな機能部を追加することが可能である。

【００７５】

外部機器制御部１１０は，サービス制御部１６により起動され，サービス制御部１６から通知された情報に基づき，該当するネットワーク機器に対して制御コマンドを送出する。図９は，外部機器制御部１１０の処理フローを示すフローチャートである。

【００７６】

外部機器制御部１１０は，サービス制御部１６から通知された情報に基づき，制御すべきネットワーク機器を特定し，サービス制御部１６から通知された情報と，ＣＬＩライブラリ１１２とを用いて，特定されたネットワーク機器に固有な制御コマンドを編集する（Ｓ３１）。

【００７７】

続いて，外部機器制御部１１０は，特定されたネットワーク機器（外部機器）に対して編集したコマンドを，ＣＬＩライブラリ１１２を用いてネットワーク機器に固有なプロトコル（例えばTelnet）で送信する（Ｓ３２）。

【００７８】

最後に，外部機器制御部１１０は，ネットワーク機器へのコマンドの送信（設定）が成功した場合に，設定対象となったユーザ端末のＩＰアドレス，後に設定情報を変更するために必要となる設定情報，設定状態，情報を設定した外部機器アドレスをアクセスリスト１１１に登録し（Ｓ３３），処理を終了する。

【００７９】

周期処理部１９は，初期設定処理部１２により最初に起動され，以降，周期的にシグナル割り込み等の手法を用いて起動される。周期処理部１９は，アクセスリスト１１１のエントリに設定されたタイマを管理し，タイマが満了した場合に，サービス制御部１６にタイマ満了イベントを通知する。図１０は，周期処理部１９の処理フローを示すフローチャートである。

【００８０】

周期処理部１９は，アクセスリスト１１１を読み込み（Ｓ４１），アクセスリストエントリに設定されているタイマを減算する（Ｓ４２）。

【００８１】

続いて，周期処理部１９は，タイマが満了しているかどうかを調べ（Ｓ４３），満了している場合には（Ｓ４３でＹＥＳ），アクセスリスト１１１のエントリに設定されている情報に基づいてタイムアウトイベントを生成し，サービス制御部１６を起動する（Ｓ４４）。一方，タイマが満了していない場合には，周期処理部１９は，ステップＳ４４の処理をスキップする。

【００８２】

続いて，周期処理部１９は，アクセスリスト１１１の全てのエントリの処理が終了しているかどうかを判断し（Ｓ４５），すべてのエントリの処理が終了している場合には，処理を終了し，終了していない場合には，ステップＳ４１～Ｓ４４の処理を繰り返す。

【００８３】

次に，ＰＮＣＵ１の利点を示すために，ＰＮＣＵ１をいくつかのサービスに適用した適用例について，それを従来の技術で解決した場合と比較しながら説明する。

【００８４】

＜第１の適用例＞

第１の適用例として，ＤＨＣＰ（Dynamic Host Configuration Protocol）サーバを利用したネットワークにおいて，ＰＮＣＵ１によりアクセス規制を行うサービス例について説明する。

【００８５】

図１１は，ＤＨＣＰサーバによるユーザ端末へのアドレス割り当て（払い出し）を行う場合におけるネットワークのセキュリティ上の問題点の説明図であり，図１１（Ｂ）は，この問題点を従来技術により解決する場合のネットワークシステムの構成図である。また，図１１（Ｃ）は，ＰＮＣＵ１によりこの問題点を解決する場合のネットワークシステムの構成図である。

【００８６】

ＰＮＣＵ１は，前述したように，図１（Ａ）～（Ｄ）のいずれかの構成でネットワークに組み込むことができるが，図１１（Ｃ）では，一例として図１（Ｃ）に示す構成例３による構成のみを示している。

【００８７】

図１１（Ａ）では，ＤＨＣＰサーバ２ａ～２ｃおよび認証サーバ６が図１（Ａ）～（Ｄ）のサービスサーバ２に対応し，Ｌ３ＳＷ４１が図１（Ａ）～（Ｄ）のネットワーク機器４１に対応する。また，ユーザ端末３ａおよび３ｂが図１（Ａ）～（Ｄ）のユーザ端末３に対応する。

【００８８】

まず図１１（Ａ）を参照して，ＤＨＣＰサーバ２ａを運用しているネットワークでは，通常，ユーザ端末３ａのようにＤＨＣＰを利用するユーザ端末は，ＤＨＣＰサーバ２ａからＩＰアドレスやその他の情報を自動的に取得し，ネットワーク４にアクセスする。

【００８９】

ＤＨＣＰサーバ２ａは，一般に，登録されたユーザ端末のみにＩＰアドレスを割り当てる（払い出す）機能を有する。ネットワークに接続する全てのユーザ端末がＤＨＣＰを利用するように設定されていれば，ＤＨＣＰサーバ２ａに登録されていないユーザ端末には，ＤＨＣＰサーバ２ａからＩＰアドレスが払い出されない。したがって，不正にアクセスしようとするユーザ端末は，ＩＰアドレスを取得できず，ネットワークにアクセスできない。

【００９０】

しかし，不正にアクセスしようとするユーザ端末３ｂが，ＤＨＣＰサーバ２ａが払い出す情報を何らかの手段で知ることができた場合に，ユーザ端末３ｂは，ＤＨＣＰを利用せずに，ＩＰアドレスやデフォルトルートを直接設定することにより，ネットワークに接続し通信を行うことができる。これは，ユーザ端末が接続したローカルネットワークと外部ネットワークとを接続するネットワーク機器（ここではＬ３ＳＷ４１）にＤＨＣＰサーバ２ａが払い出したＩＰアドレスのみを通過させるような規制が設定されていないからである。

【００９１】

これを解決する方法としては，図１１（Ｂ）に示すように，ＤＨＣＰサーバ，認証サーバ，およびファイアウォール（ＦＷ）を組み合わせて，ＤＨＣＰサーバが払い出したＩＰアドレスのみを通過可能とする方法が提案されている。

【００９２】

まず，ＤＨＣＰを利用するユーザ端末３ａは，認証サーバ６と通信するための仮のアドレスをＤＨＣＰサーバ２ｂから取得する。続いて，ユーザ端末３ａは，この仮のアドレスを利用して認証サーバ６にアクセスして認証を受ける。

【００９３】

認証後，ユーザ端末３ａは，ネットワークにアクセスして通信するための正規のアドレスの払い出しをＤＨＣＰサーバ２ｂに要求する。ＤＨＣＰサーバ２ｂは，認証サーバ６と連携しており，アドレス払い出しを要求したユーザ端末３ａが認証済みかどうかを認証サーバ６に確認する。

【００９４】

ユーザ端末３ａが認証済みである場合には，ＤＨＣＰサーバ２ｂは，ＦＷ７に対して，ユーザ端末３ａに払い出す正規のアドレスの規制解除を行うように設定し，ユーザ端末３ａにこの正規のアドレスを払い出す。

【００９５】

一方，ＤＨＣＰを利用しないユーザ端末３ｂは，ＤＨＣＰサーバ２ｂによって払い出されたアドレスを有しないので，ＦＷ７を通過することができず，ネットワークにアクセスして通信を行うことができない。

【００９６】

このように，従来の方法により問題を解決する場合には，ＤＨＣＰサーバ２ｂとして，ＦＷ７の設定を行うことができる特殊なものが必要であり，また，ＦＷ７も，ＤＨＣＰサーバ２ｂにより設定を受けることができる特殊なものが必要である。したがって，ＦＷを導入することにより，ＤＨＣＰサーバを特殊なものに交換したり，あるいは，ＦＷと組み合わせて使用できるＤＨＣＰサーバに取り替えたりする必要がある。なお，別の方式としては認証サーバとＦＷが連携する方式もあるが，この場合も認証サーバとして特殊なものが必要となる。したがって，既存の装置をそのまま使用することができない。

【００９７】

これに対して，ＰＮＣＵ１を利用する場合には，図１１（Ｃ）に示すように，Ｌ３ＳＷ４１にＰＮＣＵ１を接続するだけでアクセス規制を行うことができ，ＤＨＣＰサーバ２ｃおよび認証サーバ５（ならびにＬ３ＳＷ４１）は既存のものを使用することができる。

【００９８】

図１１（Ｃ）では，ＦＷを使用せず，ＤＨＣＰサーバ２ｃ，認証サーバ６，およびＬ３ＳＷ４１を用いてアクセス規制を行う例を示している。ここで，Ｌ３ＳＷ４１は，設定されたアドレスのパケットのみを通過させる機能を有するものとする。

【００９９】

まず，ＤＨＣＰを利用するユーザ端末３ａは，認証サーバ６と通信するための仮のアドレスをＤＨＣＰサーバ２ｃから取得する。続いて，ユーザ端末３ａは，

この仮のアドレスを使用して認証サーバ６にアクセスし，認証を受ける。

【０１００】

認証後，ユーザ端末３ａは，ＤＨＣＰサーバ２ｃに正規のアドレスの払い出しを要求する。ＤＨＣＰサーバ２ｃは認証サーバ６と連携しており，アドレス払い出しを要求したユーザ端末３ａが認証済みかどうかを認証サーバ６に確認する。認証済みであれば，ＤＨＣＰサーバ２ｃは，ユーザ端末３ａに対して正規のアドレスを払い出す。

【０１０１】

ＰＮＣＵ１は，Ｌ３ＳＷ４１の監視インタフェースに接続され，Ｌ３ＳＷ４１を通過する全てのパケットを監視している。そして，ＰＮＣＵ１は，払い出されたアドレスを含んだ応答メッセージを捕捉すると，応答メッセージを解析する。

【０１０２】

応答メッセージが正常であり，正規のアドレスを含んでいる場合には，ＰＮＣＵ１は，応答メッセージに含まれる正規のアドレスの規制解除を行うように，Ｌ３ＳＷ４１を設定する。

【０１０３】

一方，ＤＨＣＰを利用しないユーザ端末３ｂは，前述したように，ＤＨＣＰサーバ２ｃによってアドレスの払い出しを受けていないので，Ｌ３ＳＷ４１を通過することができず，ネットワークへアクセスすることができない。

【０１０４】

このように，ＰＮＣＵ１を用いて実現する場合の長所は，特殊なＤＨＣＰサーバ，認証サーバ，ファイアウォール等をネットワークに導入することなく，ファイアウォールと同等のアクセス機能を持つネットワーク機器（例えばＬ３ＳＷ）がネットワークに既にあれば，それを利用して，アクセス規制を行うことができることである。さらに，本発明の方式ではＤＨＣＰサーバが認証サーバと連携せずにＭＡＣアドレス認証等の簡単な認証機能しか持っていない場合にも対応可能である。

【０１０５】

図１１（Ｃ）のＰＮＣＵ１を用いたＤＨＣＰ手順と連携したアクセス制御につ

いて，以下により具体的に説明する。

【０１０６】

図１２（Ａ）はアドレスリスト１１の一例を，図１２（Ｂ）はサービス管理テーブル１４の一例を，図１２（Ｃ）はアクセスリスト１１１の一例を，それぞれ示している。

【０１０７】

ＰＮＣＵ１を起動すると，前述したように，まず初期設定処理部１２が起動され，アドレスリスト１１が初期設定処理部１２に読み込まれる（図６のＳ１）。

【０１０８】

アドレスリスト１１（図１２（Ａ）参照）には，サービスタイプとしてＤＨＣＰが登録され，サービス固有情報としてＤＨＣＰサーバが払い出すＩＰアドレスの一覧が登録されている。

【０１０９】

サービスタイプがＤＨＣＰであるので，初期設定処理ブロック１２は，サービス管理テーブル１４（図１２（Ｂ）参照）のＤＨＣＰ処理決定テーブルをイベント＝“初期設定”で索引し（図６のＳ２），索引先に示されている処理実体（例えばDHCP_INITで示されるプログラム）を実行する（図６のＳ３）。

【０１１０】

図１３は，DHCP_INITの処理フローを示すフローチャートである。DHCP_INITの処理では，パケット監視部１３のパケット監視条件が設定される（Ｓ５１）。具体的な設定条件は，ＵＤＰパケットの宛先ポート番号６７(bootp server)，６８（bootp client）である。

【０１１１】

次に，アドレスリスト１１（図１２（Ａ）参照）のＩＰアドレス一覧における各ＩＰアドレスに対して，外部機器制御部１１０が起動されて，初期設定の規制情報が設定される（Ｓ５２）。設定する情報は，例えばＤＮＳ（Domain Name System），ＤＨＣＰ以外の全てのパケットの規制である。

【０１１２】

ＤＨＣＰ固有の初期設定処理が終了すると，初期設定処理部１２は，パケット

監視部１３および周期処理部１９を起動する（図６のＳ５，Ｓ６）。

【０１１３】

パケット監視部１３は，監視インタフェースが受信する全てのパケットを監視し（図７のＳ１１），監視条件に一致するパケットを受信すると，サービス制御部１６を起動する（図７のＳ１２～Ｓ１４）。監視条件はＵＤＰ宛先ポート番号６７，６８である。ＵＤＰ宛先ポート番号６７に一致するものは図１６のシーケンス図におけるDHCPDISCOVERとDHCPREQUESTである。ＵＤＰ宛先ポート番号６８に一致するものはシーケンス図におけるDHCPOFEERとDHCPACKである。

【０１１４】

サービス制御部１６は，受信したパケットのＵＤＰ宛先ポート番号が６７または６８であることにより，そのパケットがＤＨＣＰのメッセージであることを識別する。そして，サービス制御部１６は，図１８（Ａ）に示すフォーマットを有するＤＨＣＰメッセージのＤＨＣＰメッセージタイプオプション（図１８（Ｃ）参照）を参照してイベントを決定する。

【０１１５】

メッセージタイプがDHCPACKである場合には，サービス制御部１６は，イベントをアドレス払い出しに決定する（図８のＳ２１）。また，サービスタイプがＤＨＣＰであるので，サービス制御部１６は，サービス管理テーブル１４（図１２（Ｂ）参照）のＤＨＣＰ処理決定テーブルをイベント＝“アドレス払い出し”で索引する（図８のＳ２２）。索引先に示されている処理実体（例えばプログラムDHCP_SET）の処理を行う（図８のＳ２３）。

【０１１６】

図１４は，DHCP_SETの処理フローを示すフローチャートである。DHCP_SETでは，まず，受信したDHCPACKメッセージが解析され，必要情報が抽出される（Ｓ５３）。すなわち，ＤＨＣＰサーバからユーザ端末に払い出されたＩＰアドレスが，図１８（Ａ） のyiaddrフィールドから抽出され，ＩＰアドレスの有効時間が，図１８（Ｂ）のIP Address Lease Timeフィールドから抽出される。

【０１１７】

続いて，抽出されたＩＰアドレスおよび有効時間をパラメータにして，外部機

器制御部１１０が起動され，外部機器制御部１１０は，ＩＰアドレスに該当する外部機器（Ｌ３ＳＷ４１）の規制解除を行う（Ｓ５４）。例えば，ＩＰアドレスに該当する外部機器の全てのプロトコルの規制解除が行われる。

【０１１８】

外部機器制御部１１０は，DHCP_SETから渡されたパラメータに基づいて，外部機器に設定するコマンドを編集する（図９のＳ３１）。続いて，外部機器制御部１１０は，DHCP_SETから渡されたＩＰアドレスのネットワークプレフィックスまたは予め登録されている機器情報に基づき，制御コマンドを送出する外部機器を決定し，外部機器へコマンドが送出する（図９のＳ３２）。

【０１１９】

制御コマンドの設定手順が終了すると，外部機器制御部１１０は，アクセスリスト１１１（図１２（Ｃ）参照）に設定内容を登録する（図９のＳ３３）。具体的には，ＩＰアドレスの欄にユーザ端末のＩＰアドレスを，状態の欄に「規制無し」を，外部機器アドレスの欄に規制情報を設定した外部機器のＩＰアドレスを，タイマの欄にアドレスの有効時間を，それぞれ設定する。

【０１２０】

アドレス返却時には，以下の処理が実行される。

【０１２１】

パケット監視部１３のパケットの監視条件は，上記同様に，ＵＤＰ宛先ポート番号６７，６８である。図１８のシーケンス図に示すように，アドレス返却時にユーザ端末からＤＨＣＰサーバに送信されるメッセージDHCPRELEASEはＵＤＰポート番号６７を有する。

【０１２２】

サービス制御部１６は，受信したパケットがＵＤＰ宛先ポート番号６７を有することにより，そのパケットがＤＨＣＰのメッセージであることを識別し，ＤＨＣＰメッセージのＤＨＣＰメッセージタイプオプション（図１８（Ｃ）参照）を参照してイベントを決定する。

【０１２３】

続いて，サービス制御部１６は，メッセージタイプがDHCPRELEASEであればイ

ベントをアドレス解放に決定する（図８のＳ２１）。サービスタイプがＤＨＣＰであるので，サービス制御部１６は，サービス管理テーブル１４（図１２（Ｂ）参照）のＤＨＣＰ処理決定テーブルを，イベント＝“アドレス解放”で索引し（図８のＳ２２），索引先に示されている処理実体（例えばプログラムDHCP_REL）の処理を行う（図８のＳ２３）。

【０１２４】

図１５は，DHCP_RELの処理フローを示すフローチャートである。DHCP_RELでは，まず，受信したDHCPRELEASEメッセージが解析され，メッセージから必要な情報が抽出される（Ｓ５５）。すなわち，図１８（Ａ）のciaddrフィールドから，解放するＩＰアドレスが抽出される。抽出されたＩＰアドレスをパラメータにして，外部機器制御部１１０が起動され，ＩＰアドレスに該当する外部機器の規制解除が行われる（Ｓ５６）。初期設定時と同じ規制条件が設定される。

【０１２５】

外部機器制御部１１０は，DHCP_RELから渡されたパラメータに基づいて，外部機器に設定するコマンドを編集する（図９のＳ３１）。また，外部機器制御部１１０は，DHCP_RELから渡されたＩＰアドレスのネットワークプレフィックスまたは予め登録されている機器情報に基づき制御コマンドを送出する外部機器を決定し，外部機器へコマンドを送出する（図９のＳ３２）。

【０１２６】

制御コマンドの設定手順が終了すると，外部機器制御部１１０は，アクセスリスト設定内容を変更する（図９のＳ３３）。具体的には，該当するＩＰアドレスエントリの状態の欄に「規制有り」が設定され，アドレスの有効時間の欄に「無効」が設定される。

【０１２７】

周期処理部１９の処理により，アドレスのリリース期間の満了に伴うアクセス規制を設定することもできる。

【０１２８】

周期処理部１９は，周期的にアクセスリストを監視し，設定されているタイマを減算する。タイマが満了している場合には，周期処理部１９は，アクセスリス

ト１１１のエントリの設定情報に基づいてタイマ満了イベントをサービス制御部１６に通知する（図１０のＳ４１～Ｓ４４）。

【０１２９】

サービス制御部１６は，通知されたタイマ満了イベントにより，サービスタイプ＝“ＤＨＣＰ”，イベント＝“タイムアウト”を決定する（図８のＳ２１）。そして，サービス制御部１６は，サービスタイプがＤＨＣＰであるので，サービス管理テーブル５４のＤＨＣＰ処理決定テーブルをイベント＝“タイムアウト”で索引し（図８のＳ２２），索引先に示されている処理実体（例えばプログラムDHCP_REL）の処理を行う（図８のＳ２３）。

【０１３０】

以降の処理は，情報をDHCPRELEASEメッセージではなく，内部イベント情報（タイマ満了イベント）から抽出する点を除き，上記のDHCPRELEASEメッセージの処理と同様である。

【０１３１】

このように，ＰＮＣＵ１を用いることで，既存のネットワーク資源を変更することなく，ＤＨＣＰ手順と連携したアクセス規制サービスを行うことができる。

【０１３２】

なお，前述したように，ＰＮＣＵ１は，図１（Ａ），（Ｂ），または（Ｄ）に示す構成でネットワークに接続され，または，ＤＨＣＰサーバ２ｃに内蔵されてもよい。ＰＮＣＵ１がＤＨＣＰサーバ２ｃに内蔵される場合には，ＰＮＣＵ１の機能をプログラムにより実現してＤＨＣＰサーバ２ｃに格納し，ＤＨＣＰサーバ２ｃのＣＰＵによりこのプログラムを実行させることもできる。

【０１３３】

＜第２の適用例＞

第２の適用例は，移動通信プロトコルMobile IPv4におけるファイアウォール（ＦＷ）のパケット通過規制解除にＰＮＣＵ１を適用したものである。

【０１３４】

図１９（Ａ）は，Mobile IPv4においてＦＷを設置した場合に発生する問題点の説明図であり，図１９（Ｂ）は，この問題点を従来技術により解決する場合の

ネットワークシステムの構成図である。また，図１９（Ｃ）は，ＰＮＣＵ１によりこの問題点を解決する場合のネットワークシステムの構成図である。

【０１３５】

ＰＮＣＵ１は，図１（Ａ）～（Ｄ）のいずれかの構成でネットワークに組み込むことができるが，図１９（Ｃ）では，一例として図１（Ｃ）に示す構成例３による構成のみを示している。

【０１３６】

図１９（Ａ）～（Ｃ）において，ユーザ端末３は，移動端末（携帯電話等）であり，ホームエージェント（ＨＡ：Home Agent）８のホームネットワークのアドレスをホームアドレスとして有する。ルータ４２は，外部ネットワーク（Foreign Network）に配置されたネットワーク機器であり，外部エージェント（ＦＡ：Foreign Agent）であってもよい。ルータ４２とネットワーク４との間には，ファイアウォール（ＦＷ）７ａまたは７ｂが接続されている。ユーザ端末３は，ホームネットワークから外部ネットワークに移動している。

【０１３７】

図１９（Ａ）において，ＦＷ７ａは，ルータ４２からネットワーク４に向けて（すなわち外部ネットワークからネットワーク４に向けて）送信されるパケットの送信元アドレスをチェックし，その送信元アドレスが外部ネットワーク内に本来存在しないアドレスである場合には，そのパケットを通過させないように設定されることがある。

【０１３８】

ユーザ端末３は，ホームアドレスと外部ネットワークで取得する気付アドレス（Care-of Address）とを保持する。ユーザ端末３が，ホームアドレスと気付アドレスとの対応をＨＡ８に登録するときは，気付アドレスを用いて通信が行われる一方，ユーザ端末３が電子メール等の通常のデータパケットを送信するときは，ＩＰパケットの始点アドレスがホームアドレスに設定される。

【０１３９】

したがって，前述のようなＦＷの設定が行われていると，アドレスの対応をＨＡ８に登録する際に送信されるパケットはＦＷ７ａを通過することができる一方

，通常のデータベースパケットはＦＷ７ａを通過することができず，ユーザ端末３は相手端末と通信を行うことができないという問題が発生する。

【０１４０】

この問題を解決するために，ユーザ端末３が送信するＩＰパケットを気付アドレスでカプセル化したり，ＦＷ７ａの設定を動的に変えたりする方法が提案されている。

【０１４１】

図１９（Ｂ）は，従来技術による問題の解決方法として，ＦＷ７ｂの設定を動的に変える方法を示している。ＦＷ７ｂは，通過するパケットを監視し，Mobile IPv4の位置登録応答メッセージであるRegistration Replyメッセージを捕捉し，このメッセージ内の結果コードとホームアドレスとを参照して，結果が正常終了であれば，ホームアドレスのアクセス規制を解除する設定を行う。

【０１４２】

また，他の実現手段としては，認証サーバと連携して認証サーバがＦＷの穴あけを行う方式もある。

【０１４３】

いずれの方法でも，特殊なファイアウォールか，特定の認証サーバとファイアウォールの組み合わせをネットワークに設置する必要があり，これまでMobile IPv4を適用していなかったネットワークでは，ネットワーク構成の変更無しではファイアウォール通過のための機能を追加できないこととなる。

【０１４４】

これに対して，ＰＮＣＵ１を利用する場合には，図１９（Ｃ）に示すように，ルータ４２にＰＮＣＵ１を接続するだけで，ファイアウォール通過の問題点を解決することができ，ＦＷとして特殊なものを使用する必要もなく，ネットワークの構成を変更する必要もない。

【０１４５】

図１９（Ｃ）では，ＰＮＣＵ１は，ルータ４２を通過するパケット（Mobile IPv4のメッセージ）を監視し，ユーザ端末３のホームアドレスを取得する。そして，ＰＮＣＵ１は，ユーザ端末３のホームアドレスを有するパケットを通過させ

るようにＦＷ７ａを制御する。

【０１４６】

したがって，ＰＮＣＵ１を利用することにより，ＦＷ７ａを特殊なものに取り替える必要もなく，またネットワーク構成を変える必要もない。

【０１４７】

図１９（Ｃ）に示すＰＮＣＵ１を用いたMobile IPv4のファイアウォール通過問題の解決方法について，以下に，より具体的に説明する。

【０１４８】

図２０（Ａ）はアドレスリスト１１の一例を，図２０（Ｂ）はサービス管理テーブル１４の一例を，図２０（Ｃ）はアクセスリスト１１１の一例を，それぞれ示している。

【０１４９】

ＰＮＣＵ１を起動すると，前述したように，まず初期設定処理部１２が起動され，アドレスリスト１１が読み込まれる（図６のＳ１）。アドレスリスト１１（図２０（Ａ）参照）には，サービスタイプとしてMobileIPv４が登録されている。サービス固有情報は存在しない。サービスタイプがMobileIPv４であるので，初期設定処理部１２は，サービス管理テーブル１４のMobile IPv４処理決定テーブルをイベント＝“初期設定”で索引する（図６のＳ２）。

【０１５０】

続いて，初期設定処理部１２は，索引先に示されている処理実体（たとえばプログラムMobileIP_INIT）の処理を行う（図６のＳ３）。

【０１５１】

図２１は，MobileIP_INITの処理フローを示すフローチャートである。MobileIP_INITでは，パケット監視部１３がパケットを監視するための条件が設定される（Ｓ６１）。具体的な設定条件は，ＵＤＰパケットの送信元と宛先ポート番号４３４（Mobile IPv4）である。

【０１５２】

ＭｏｂｉｌｅＩＰの初期設定処理を終了すると，初期設定処理部１２は，パケット監視部１３および周期処理部１９を起動する（図６のＳ５，Ｓ６）。

【０１５３】

パケット監視部１３は，監視インタフェースにより受信される全てのパケットを監視し（図７のＳ１１），監視条件に一致するパケットを受信すると，サービス制御部１６を起動する（図７のＳ１２～Ｓ１４）。監視条件はＵＤＰ送信元と宛先ポート番号４３４である。宛先ポート番号４３４に一致するパケットは，図２４に示すMobile IPv4の位置登録シーケンス図におけるRegistration Requestであり，送信元ポート番号４３４に一致するパケットはRegistration Replyである。

【０１５４】

サービス制御部１６は，受信パケットのＵＤＰ送信元，宛先ポート番号４３４より，受信パケットがMobile IPのメッセージであることを識別し，Mobile IPv４メッセージのメッセージタイプ（Type）（図２５（Ａ）および（Ｂ）参照）を参照してイベントを決定する。

【０１５５】

メッセージタイプがRegistration Replyである場合には，サービス制御部１６は，イベントを位置登録応答に決定する（図８のＳ２１）。サービスタイプはMobile IPv4であるので，サービス制御部１６は，サービス管理テーブル１４（図２０（Ｂ）参照）のMobile IPv4処理決定テーブルをイベント＝“位置登録応答”で索引する（図８のＳ２２）。続いて，サービス制御部１６は，索引先に示されている処理実体（例えばプログラムMobileIP_REP）の処理を行う（図８のＳ２３）。

【０１５６】

図２２は，MobileIP_REPの処理フローを示すフローチャートである。MobileIP_REPでは，まず，受信したRegistration Replyメッセージが解析され，必要な情報が抽出される（Ｓ６２）。

【０１５７】

すなわち，位置登録の処理結果が図２５（Ｂ）のCodeフィールドから抽出され，規制を解除する端末のＩＰアドレスが図２５（Ｂ）のHome Addressフィールドから抽出される。また，位置登録の有効時間が図２５（Ｂ）のLifetimeフィール

ドから抽出される。

【０１５８】

Codeフィールドの値が正常応答を示す値（すなわち０）である場合には（Ｓ６３で０），外部機器制御部１１０が起動され，ＩＰアドレスに対応する外部機器の規制解除が行われる（Ｓ６４）。一方，Codeフィールドの値が正常応答を示す値（すなわち０）でない場合には（Ｓ６３で≠０），処理は終了する。

【０１５９】

抽出されたＩＰアドレスと有効時間をパラメータにして，設定される情報は，例えばＩＰアドレスに対する全てのプロトコルの規制解除である。

【０１６０】

外部機器制御部１１０は，MobileIP_REPより渡されたパラメータから，外部機器に設定するコマンドを編集する（図９のＳ３１）。続いて，外部機器制御部１１０は，予め登録されている機器情報に基づいて，制御コマンドを送出する外部機器を決定し，外部機器へコマンドを送出する（図９のＳ３２）。

【０１６１】

制御コマンドの設定手順が終了すると，アクセスリスト１１１に設定内容を登録する（図９のＳ３３）。具体的には，ＩＰアドレスの欄にユーザ端末のＩＰアドレスが設定され，状態の欄に規制無しが設定される。また，外部機器アドレスの欄に，規制情報を設定した外部機器のＩＰアドレスが設定され，タイマにアドレスの有効時間が設定される。

【０１６２】

Mobile IPの明示的な終了手順は，図２４に示す位置登録シーケンス図において，Registration RequestメッセージのLifetimeフィールド（図２５（Ａ）参照）を０に設定したメッセージを送信することにより行われる。

【０１６３】

サービス制御部１６は，受信パケットのＵＤＰ送信元，宛先ポート番号４３４より，受信パケットがMobile IPのメッセージであることを識別し，Mobile IPv4メッセージのメッセージタイプを参照してイベントを決定する。

【０１６４】

メッセージタイプがRegistration Requestであれば，サービス制御部１６はイベントが位置登録要求であると判断する（図８のＳ２１）。サービスタイプはMobile IPv4であるので，サービス制御部１６は，サービス管理テーブル１４（図２０（Ｂ）参照）のMobile IPv4処理決定テーブルをイベント＝“位置登録要求”で索引する（図８のＳ２２）。

【０１６５】

続いて，サービス制御部１６は，索引先に示されている処理実体（例えばプログラムMobileIP_REQ）の処理を行う（図８のＳ２３）。

【０１６６】

図２３は，MobileIP_REQの処理フローを示すフローチャートである。MobileIP_REQでは，まず，受信したRegistration Requestメッセージが解析され，対象とするユーザ端末のＩＰアドレスがHome Addressフィールドから抽出され，位置登録の有効時間がLifetimeフィールドから抽出される（Ｓ６５）。

【０１６７】

有効時間が０であるならば（Ｓ６６で０），外部機器制御部１１０が起動され，ＩＰアドレスの規制が行われる（Ｓ６７）。設定する情報は，該当ＩＰアドレスに対する規制解除条件の解除である。

【０１６８】

外部機器制御部１１０は，MobileIP_REQから渡されたパラメータに基づいて，外部機器に設定するコマンドを編集する（図９のＳ３１）。続いて，外部機器制御部１１０は，予め登録されている機器情報に基づき，制御コマンドを送出する外部機器を決定し，外部機器へコマンドを送出する（図９のＳ３２）。制御コマンドの設定手順が終了すると，外部機器制御部１１０は，アクセスリスト設定内容を削除する（図９のＳ３３）。

【０１６９】

ライフタイム満了に伴うアクセス規制の設定も行われる。周期処理部１９は，周期的にアクセスリスト１１１を監視し，設定されているタイマを減算する。タイマが満了している場合には，周期処理部１９は，アクセスリスト１１１のエントリ設定情報に基づいて，タイマ満了イベントをサービス制御部１６に通知する

（図１０のＳ４１～Ｓ４４）。

【０１７０】

サービス制御部１６は，通知されたタイマ満了イベントにより，サービスタイプ＝“MobileIP”，イベント＝“タイムアウト”を決定する（図８のＳ２１）。サービスタイプがＭｏｂｉｌｅＩＰであるので，サービス制御部１６は，サービス管理テーブル１４（図２４）のＭｏｂｉｌｅＩＰ処理決定テーブルをイベント＝“タイムアウト”で索引する（図８のＳ２２）。索引先に示されている処理実体（例えばプログラムMobileIP_REL）の処理を行う（図８のＳ２３）。

【０１７１】

以降の処理は，情報を，Registration Requestメッセージではなく，内部イベント情報（タイマ満了イベント）から抽出する点を除き，上記のRegistration Requestメッセージについての処理と同様である。

【０１７２】

このように，ＰＮＣＵ１を用いることで，特殊なファイアウォールをネットワークに導入することなく，Mobile IPv4を用いるユーザ端末の接続が可能になる。

【０１７３】

＜第３の適用例＞

第３の適用例は，ＩＰｖ６におけるアクセス規制にＰＮＣＵ１を適用したものである。

【０１７４】

図２６（Ａ）は，ＩＥＴＦ（Internet Engineering Task Force）で提案されているＩＰｖ６におけるアクセス規制方式の概要を示している。ＩＰｖ６では，ＩＰｖ４と同じようにＤＨＣＰサーバを用いてアドレスを生成するステートフルアドレス構成方法と，ルータからのネットワークプレフィックスの広告と端末の識別子を組み合わせることでアドレスを自動生成するステートレスアドレス構成方法との２つのアドレス自動構成方法が提案されている。このようなアドレス自動構成では，第１の適用例で示したＩＰｖ４のＤＨＣＰと同じセキュリティ上の問題が生じる。

【０１７５】

この解決方法として，アドレス自動生成時に認証手順を絡めることで，認証が成功したユーザ端末のみがネットワークにアクセス可能になるような方式が提案されている。この方式を，ステートレスアドレス自動構成方法を例にとり具体的に説明する。

【０１７６】

ユーザ端末（ＩＰｖ６端末）３は，ネットワーク機器であるアテンダント（ルータ）４３から広告されたネットワークプレフィックスとユーザ端末３の識別子とに基づいてＩＰｖ６アドレスを生成する。

【０１７７】

アドレス生成後，ユーザ端末３は，生成したアドレスの認証要求をテンダント４３に送信する。アテンダント４３は，認証サーバ９との間で交換される認証プロトコルに基づいて，認証要求を認証サーバ９に転送する。認証サーバ９は，認証結果をアテンダント４３に返信する。アテンダント４３は，認証結果が認証成功であれば，ユーザ端末３が提示したＩＰｖ６アドレスのフィルタ規制を解除し，ユーザ端末３へ認証応答メッセージを返信する。

【０１７８】

ＩＰｖ６で提案されている方式では，アテンダントと呼ばれる特殊なルータが必要となるが，現状このような機能を持ったルータは存在せず，このようなネットワーク構成が広まるにはかなりの時間を要することが予想される。

【０１７９】

しかし，セキュリティ（アクセス規制）の問題は早急に解決する必要がある。本発明によれば，ＩＰｖ６ネットワーク上に，アテンダントと呼ばれる装置の一部の機能を確保し，あるいはそのような機能がない場合でも同様のセキュリティを確保することが可能となる。

【０１８０】

図２６（Ｂ）は，アテンダント４３は存在するが，アテンダント４３にアクセス規制を行う機能が無い場合のネットワーク構成例を示すブロック図である。この場合に，ＰＮＣＵ１は，第１の適用例のＤＨＣＰの場合と同様に，認証応答メ

ッセージを捕捉することにより，アテンダント４３以外の別のアクセス規制機能を持つネットワーク機器（図２６（Ｂ）のＬ３ＳＷ４１）に対してアクセス規制を設定できる。

【０１８１】

図２６（Ｃ）は，アクセス規制機能を持つネットワーク機器（Ｌ３ＳＷ４１）のみが存在し，アテンダント機能そのものがない場合の例である。この場合に，ＰＮＣＵ１は，ユーザ端末３から送信される認証要求メッセージを捕捉し，ルータ４４の代わりに，認証サーバ９とのメッセージの交換，アクセス規制制御を行う。ユーザ端末３からルータ４４宛てに送信された認証要求メッセージ（オリジナルのメッセージ）はルータ４４で廃棄される。ＰＮＣＵ１は，認証処理および規制解除を行った後，ルータ４４に代わってユーザ端末３へ認証応答メッセージを返す。

【０１８２】

以下に，図２６（Ｃ）に示す，ＰＮＣＵ１を用いたＩＰｖ６アドレス自動構成と連携したアテンダントサービスの具体的な実施例を示す。

【０１８３】

ＩＰｖ６の認証に関する標準技術は，現在のところ確立されていないが，以下では，ＩＥＴＦ草案に基づくステートレスアドレス自動構成を例として説明する。

【０１８４】

図２７（Ａ）はアドレスリスト１１の一例を，図２７（Ｂ）はサービス管理テーブル１４の一例を，図２７（Ｃ）はアクセスリスト１１１の一例を，それぞれ示している。

【０１８５】

ＰＮＣＵ１を起動すると，既に説明したように，まず初期設定処理部１２が起動され，アドレスリスト１１（図２７（Ａ）参照）が読み込まれる（図６のＳ１）。アドレスリスト１１には，サービスタイプとしてＩＰｖ６が登録されている。なお，アドレスリスト１１にサービス固有情報は設けられていない。

【０１８６】

サービスタイプがＩＰｖ６であるので，初期設定処理部１２は，サービス管理テーブル１４（図２７（Ｂ）参照）のＩＰｖ６処理決定テーブルをイベント＝“初期設定”で索引する（図６のＳ２）。続いて，初期設定処理部１２は，索引先に示されている処理実体（例えばプログラムIPV6_INIT）の処理を行う（図６のＳ３）。

【０１８７】

図２８は，IPV6_INITの処理フローを示すフローチャートである。IPV6_INITでは，パケット監視部１３のパケット監視条件が設定される（Ｓ７１）。具体的な設定条件は，ヘッダタイプ（プロトコル）＝ＩＣＭＰである。

【０１８８】

ＩＰｖ６固有の初期設定処理が終了すると，パケット監視部１３および周期処理部１９が起動される（図６のＳ５，Ｓ６）。

【０１８９】

パケット監視部１３は，監視インタフェースにより受信される全てのパケットを監視し（図７のＳ１１），条件に一致するパケットが受信されると，サービス制御部１６を起動する（図７のＳ１２～Ｓ１４）。

【０１９０】

図３１は，ＩＰｖ６の認証シーケンス図であり，この図に示すＩＣＭＰメッセージは全て監視条件に一致する。

【０１９１】

サービス制御部１６は，受信パケットがＩＰｖ６メッセージであることを識別し，図３２に示すICMP AAAメッセージのパケット構成におけるメッセージタイプを参照してイベントを決定する。

【０１９２】

メッセージタイプがAAA Requestである場合には，サービス制御部１６は，イベントをアドレス払い出しに決定する（図８のＳ２１）。サービスタイプはＩＰｖ６であるので，サービス制御部１６は，サービス管理テーブル１４（図２７（Ｂ）参照）のＩＰｖ６処理決定テーブルをイベント＝“アドレス払い出し”で索引し（図８のＳ２２），索引先に示されている処理実体（例えばプログラムIPV

６_SET）の処理を行う（図８のＳ２３）。

【０１９３】

図２９は，IPV６_SETの処理フローを示すフローチャートである。IPV6_SETでは，まず，認証サーバ（ＡＡＡ：Authentication, Authorization and Accounting）９による該当ユーザの認証を受けるために，ICMP AAA Requestメッセージの各パラメータがＡＡＡプロトコルのパラメータに変換され（Ｓ７２），認証サーバ９に認証要求が行われる（Ｓ７３）。

【０１９４】

続いて，認証応答メッセージの結果コードが判定され（Ｓ７４），認証成功であれば（Ｓ７４で認証ＯＫ），抽出されたＩＰアドレスと有効時間をパラメータにして，外部機器制御部１１０が起動され，ＩＰアドレスの規制解除が行われる（Ｓ７５）。設定される情報は，例えば該当ＩＰアドレスに対する全てのプロトコルの規制解除である。

【０１９５】

外部機器制御部１１０は，IPV６_SETより渡されたパラメータから，外部機器に設定するコマンドを編集する（図９のＳ３１）。続いて，外部機器制御部１１０は，予め登録されている機器情報に基づき，制御コマンドを送出する外部機器を決定し，外部機器へコマンドを送出する（図９のＳ３２）。

【０１９６】

続いて，外部機器制御部１１０は，制御コマンドの設定手順が終了すると，アクセスリスト１１１に設定内容を登録する（図９のＳ３３）。具体的には，ＩＰアドレスの欄に端末のＩＰアドレスを，状態の欄に規制無しを，外部機器アドレスの欄に，規制情報を設定した外部機器のＩＰアドレスを，タイマの欄にアドレスの有効時間を，それぞれ設定する。

【０１９７】

最後に，ICMP AAA Replyメッセージが編集され，該当端末へ送信される（Ｓ７６）。

【０１９８】

図３３は，ＩＰｖ６の明示的な終了シーケンスを示している。サービス制御部

１６は，受信したＩＣＭＰパケットより，ICMP AAAメッセージのメッセージタイプを参照してイベントを決定する。メッセージタイプがAAA Teardownであれば，サービス制御部１６は，イベントをアドレス解放に決定する（図８のＳ２１）。サービスタイプがＩＰｖ６であるので，サービス管理テーブル１４（図２７（Ｂ）参照）のＩＰｖ６処理決定テーブルをイベント＝“アドレス解放”で索引し（図８のＳ２２），索引先に示されている処理実体（例えばプログラムIPV6_REL）の処理を行う（図８のＳ２３）。

【０１９９】

図３０は，IPV６_RELの処理フローを示すフローチャートである。IPV６_RELでは，まず，受信したAAA TeardownメッセージのパラメータがＡＡＡプロトコルに変換される（Ｓ７７）。続いて，セッションが解放される（Ｓ７８）。

【０２００】

続いて，外部機器制御部１１０が起動され，該当ＩＰアドレスの規制が行われる（Ｓ７９）。設定する情報は，該当ＩＰアドレスに対する規制解除条件の削除である。

【０２０１】

外部機器制御部１１０は，IPV６_RELから渡されたパラメータに基づいて，外部機器に設定するコマンドを編集する（図９のＳ３１）。続いて，外部機器制御部１１０は，予め登録されている機器情報に基づき，制御コマンドを送出する外部機器を決定し，外部機器へコマンドを送出する（図９のＳ３２）。制御コマンドの設定手順が終了すると，外部機器制御部１１０は，アクセスリスト１１１の設定内容を削除する（図９のＳ３３）。

【０２０２】

最後に，ICMP AAA Replyメッセージが編集され，該当端末へ送信される（図３０のＳ８０）。

【０２０３】

ライフタイム満了に伴うアクセス規制も設定される。周期処理部１９は，周期的にアクセスリスト１１１を監視し，設定されているタイマを減算する。タイマが満了している場合には，周期処理部１９は，アクセスリスト１１１のエントリ

の設定情報をもとに，タイマ満了イベントをサービス制御部１６に通知する（図１０のＳ４１～Ｓ４４）。

【０２０４】

サービス制御部１６は，通知されたタイマ満了イベントにより，サービスタイプ＝“ＩＰｖ６”，イベント＝“タイムアウト”を決定する（図８のＳ２１）。サービスタイプがＩＰｖ６であるので，サービス制御部１６は，サービス管理テーブル１４のＩＰｖ６処理決定テーブルをイベント＝“タイムアウト”で索引し（図８のＳ２２），索引先に示されている処理実体（例えばプログラムIPV６_REL）の処理を行う（図８のＳ２３）。

【０２０５】

以降の処理は，情報をICMP AAA Teardownメッセージではなく，内部イベント情報（タイマ満了イベント）から抽出する点を除き上記と同様である。

【０２０６】

このように，ＰＮＣＵ１を用いることで，基本的なＩＰｖ６機能しか有しないネットワークに対して，認証等の付加サービスを容易に追加することができる。

【０２０７】

（付記１）　ユーザ端末に所定のサービスを提供するサービス装置に代行して，該サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置であって，

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視するパケット監視部と，

前記パケット監視部により監視されたパケットに基づいて前記補完または拡張する機能を決定して実行する実行部と，

を備えている代理ネットワーク制御装置。

【０２０８】

（付記２）　ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置を制御することにより，前記サービス装置の機能を補完または拡張する機能を前記サービス装置に代行して実行する代理

ネットワーク制御装置であって，

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視するパケット監視部と，

前記パケット監視部により監視されたパケットに基づいて前記補完または拡張する機能を決定するサービス制御部と，

前記サービス制御部により決定された機能に基づいて前記ネットワーク装置を制御する外部機器制御部と，

を備えている代理ネットワーク制御装置。

【０２０９】

（付記３）　付記２において，

前記サービス装置はＤＨＣＰサーバであり，

前記パケット監視部は，前記サービス装置から前記ユーザ端末に発行されるアドレスを含んだパケットを監視し，

前記サービス制御部は，前記パケット監視部により監視されたパケットに基づいて，前記サービス装置により発行されたアドレスを送信元アドレスとして有するパケットを通過させ，それ以外のアドレスを送信元アドレスとして有するパケットを通過させないアクセス規制機能を決定し，

前記外部機器制御部は，前記アクセス規制機能を実行するように前記ネットワーク装置を制御する，

代理ネットワーク制御装置。

【０２１０】

（付記４）　付記２において，

前記ユーザ端末がホームネットワークのホームアドレスを有する移動通信端末であり，前記ネットワーク装置が前記ホームネットワークの外部ネットワークから外部に送信されるパケットのうち，所定の送信元アドレスを有するパケットを通過させ，それ以外のパケットを通過させないファイアウォールであり，

前記パケット監視部は，前記外部ネットワークに移動した前記ユーザ端末と前記ホームネットワークのホームエージェントとの間で通信される，前記ユーザ端末のホームアドレスを含んだパケットを監視し，

前記サービス制御部は，前記パケット監視部により監視されたパケットに基づいて，前記ホームアドレスを有するパケットを通過させるようにアクセス規制を解除する機能を決定し，

前記外部機器制御部は，前記アクセス規制を解除する機能を実行するように，前記ネットワーク装置を制御する，

代理ネットワーク制御装置。

【０２１１】

（付記５）　付記２において，

前記ユーザ端末がＩＰｖ６端末であり，前記サービス装置が生成された前記ユーザ端末のＩＰアドレスの認証を行う認証サーバであり，

前記パケット監視部は，前記サービス装置により認証されたＩＰアドレスを含むパケットを監視し，

前記サービス制御部は，前記パケット監視部により監視されたパケットに基づいて，前記ＩＰアドレスを送信元アドレスとして有するパケットを通過させるようにアクセス規制を解除する機能を決定し，

前記外部機器制御部は，前記アクセス規制を解除する機能を実行するように，前記ネットワーク装置を制御する，

代理ネットワーク制御装置。

【０２１２】

（付記６）　付記５において，

前記ユーザ端末のＩＰアドレスを生成して前記ユーザ端末に送信し，または，ネットワークプレフィックスを前記ユーザ端末に送信するアドレス送信部をさらに備えている，

代理ネットワーク制御装置。

【０２１３】

（付記７）　付記２において，

前記サービス制御部により決定される前記機能は，所定の情報を記録する機能を含む，

代理ネットワーク制御装置。

【０２１４】

（付記８）　付記２において，

前記サービス制御部により決定される前記機能は，所定のネットワーク装置またはサービス装置にメッセージを送信する機能を含む，

代理ネットワーク制御装置。

【０２１５】

（付記９）　コンピュータに，

ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間で通信されるパケットを監視する手順と，

前記監視したパケットに基づいて，前記サービス装置に代行して，該サービス装置の機能を補完または拡張する機能を決定して実行する手順と，

を実行させるためのプログラム。

【０２１６】

（付記１０）　ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置を制御することにより，前記サービス装置の機能を補完または拡張する機能を前記サービス装置に代行して実行するコンピュータに，

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視する手順と，

前記監視したパケットに基づいて前記補完または拡張する機能を決定する手順と，

前記決定した機能に基づいて前記ネットワーク装置を制御する手順と，

を実行させるためのプログラム。

【０２１７】

（付記１１）　ユーザ端末と通信を行い該ユーザ端末に所定のサービスを提供するサービス装置と，

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視し，所定の条件を満たすパケットに基づいて，前記サービス装置の機能を補完または拡

張する機能を実行する代理ネットワーク制御装置と，

を備えているネットワークシステム。

【０２１８】

（付記１２）　付記９において，

前記代理ネットワーク制御装置は前記サービス装置に内蔵されている，ネットワークシステム。

【０２１９】

（付記１３）　ユーザ端末と通信を行い該ユーザ端末に所定のサービスを提供するサービス装置と，

前記ユーザ端末と前記サービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置と，

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視し，所定の条件を満たすパケットに基づいて前記ネットワーク装置を制御することにより，前記サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置と，

を備えているネットワークシステム。

【０２２０】

（付記１４）　付記１３において，

前記代理ネットワーク制御装置は前記サービス装置に内蔵されている，ネットワークシステム。

【０２２１】

（付記１５）　付記１３において，

前記サービス装置はＤＨＣＰサーバであり，

前記代理ネットワーク制御装置は，前記サービス装置から前記ユーザ端末に配布されるアドレスを含んだパケットを監視し，前記ユーザ端末から送信される，前記アドレスを送信元アドレスとして有するパケットを通過させ，それ以外のパケットを通過させないように前記ネットワーク装置を制御する，

ネットワークシステム。

【０２２２】

（付記１６）　付記１３において，

前記ユーザ端末がホームネットワークのホームアドレスを有する移動通信端末であり，

前記ネットワーク装置は，前記ホームネットワークの外部ネットワークから外部に送信されるパケットのうち，所定の送信元アドレスを有するパケットを通過させ，それ以外のパケットを通過させないネットワーク装置であり，

前記代理ネットワーク制御装置は，前記外部ネットワークに移動した前記ユーザ端末と前記ホームネットワークのホームエージェントとの間で通信される，前記ユーザ端末のホームアドレスを含んだパケットに基づいて，前記ユーザ端末のホームアドレスを送信元アドレスとして含むパケットを通過させるように前記ネットワーク装置を制御する，

ネットワークシステム。

【０２２３】

（付記１７）　付記１３において，

前記ユーザ端末がＩＰｖ６端末であり，前記サービス装置は生成された前記ユーザ端末のＩＰアドレスの認証を行う認証サーバであり，

前記代理ネットワーク制御装置は，前記サービス装置により認証されたＩＰアドレスを送信元アドレスとして有するパケットを通過させるように前記ネットワーク装置を制御する，

ネットワークシステム。

【０２２４】

（付記１８）　付記１７において，

前記代理ネットワーク制御装置は，前記ユーザ端末のＩＰアドレスを生成して前記ユーザ端末に送信し，または，ネットワークプレフィックスを前記ユーザ端末に送信する機能をさらに実行する，

ネットワークシステム。

【０２２５】

【発明の効果】

本発明によると，既存のネットワーク構成を変更せずに，新たなネットワーク

サービスの付加機能を追加することができる。

【０２２６】

たとえば，ＤＨＣＰの運用時に問題となるセキュリティの問題を，より容易に低コストで実現することができる。また，Mobile IPv4においては，外部ネットワークに存在するユーザ端末のデータパケットがファイアウォールを通過できないといった問題を低コストで解決することができる。さらに，ＩＰｖ６のアクセス規制方式に対しても，特殊な装置を導入することなくアクセス規制の機能を提供することができる。

【０２２７】

またさらに，本発明による代理ネットワーク制御装置をネットワークに実装することにより，様々なサービスに対して機能追加が容易となる。

【図面の簡単な説明】

【図１】

（Ａ）～（Ｄ）は，本発明の実施の形態による代理ネットワーク制御装置（ＰＮＣＵ）を有するネットワークシステムの構成例を示すブロック図である。

【図２】

ＰＮＣＵの機能ブロック図である。

【図３】

アドレスリストの構成例を示す。

【図４】

サービス管理テーブルの構成例を示す。

【図５】

アクセスリストの構成例を示す。

【図６】

ＰＮＣＵの初期設定処理部の処理の流れを示すフローチャートである。

【図７】

ＰＮＣＵのパケット監視部の処理の流れを示すフローチャートである。

【図８】

ＰＮＣＵのサービス制御部の処理フローを示すフローチャートである。

【図９】

ＰＮＣＵの外部機器制御部の処理フローを示すフローチャートである。

【図１０】

ＰＮＣＵの周期処理部の処理フローを示すフローチャートである。

【図１１】

（Ａ）は，ＤＨＣＰサーバによるユーザ端末へのアドレス割り当て（払い出し）を行う場合におけるネットワークのセキュリティ上の問題点の説明図であり，（Ｂ）は，この問題点を従来技術により解決する場合のネットワークの構成図であり，（Ｃ）は，ＰＮＣＵによりこの問題点を解決する場合のネットワークシステムの構成図である。

【図１２】

（Ａ）はアドレスリストの一例を，（Ｂ）はサービス管理テーブルの一例を，（Ｃ）はアクセスリストの一例を，それぞれ示す。

【図１３】

DHCP_INITの処理フローを示すフローチャートである。

【図１４】

DHCP_SETの処理フローを示すフローチャートである。

【図１５】

DHCP_RELの処理フローを示すフローチャートである。

【図１６】

ＤＨＣＰにおけるアドレス払い出し時のメッセージフローを示すシーケンス図である。

【図１７】

ＤＨＣＰにおけるアドレス返却時のメッセージフローを示すシーケンス図である。

【図１８】

（Ａ）はＤＨＣＰメッセージのフォーマットを示し，（Ｂ）および（Ｃ）はオプションを示す。

【図１９】

（Ａ）は，Mobile IPv4においてＦＷを設置した場合に発生する問題点の説明図であり，（Ｂ）は，この問題点を従来技術により解決する場合のネットワークシステムの構成図であり，（Ｃ）は，ＰＮＣＵによりこの問題点を解決する場合のネットワークシステムの構成図である。

【図２０】

（Ａ）はアドレスリストの一例を，（Ｂ）はサービス管理テーブルの一例を，（Ｃ）はアクセスリストの一例を，それぞれ示す。

【図２１】

MobileIP_INITの処理フローを示すフローチャートである。

【図２２】

MobileIP_REPの処理フローを示すフローチャートである。

【図２３】

MobileIP_REQの処理フローを示すフローチャートである。

【図２４】

Mobile IPv4の位置登録シーケンス図である。

【図２５】

（Ａ）はMobile IPv4のRegistration Requestのパケット構成図であり，（Ｂ）はMobile IPv4のRegistration Replyのパケット構成図である。

【図２６】

（Ａ）は，ＩＥＴＦで提案されているＩＰｖ６におけるアクセス規制方式の概要を示し，（Ｂ）および（Ｃ）は，ＰＮＣＵによりアクセス規制を行う場合のネットワークシステムの構成図である。

【図２７】

（Ａ）はアドレスリストの一例を，（Ｂ）はサービス管理テーブルの一例を，（Ｃ）はアクセスリストの一例を，それぞれ示す。

【図２８】

IPV6_INITの処理フローを示すフローチャートである。

【図２９】

IPV６_SETの処理フローを示すフローチャートである。

【図３０】

IPV６_RELの処理フローを示すフローチャートである。

【図３１】

ＩＰｖ６の認証シーケンス図である。

【図３２】

ICMP AAAメッセージのパケット構成を示す。

【図３３】

ＩＰｖ６の明示的な終了シーケンスを示す。

【符号の説明】

１　ＰＮＣＵ

２　サービスサーバ

３　ユーザ端末

４　ネットワーク

４１～４ｎ　ネットワーク機器

１１　アドレスリスト

１２　初期設定処理部

１３　パケット監視部

１４　サービス管理テーブル

１６　サービス制御部

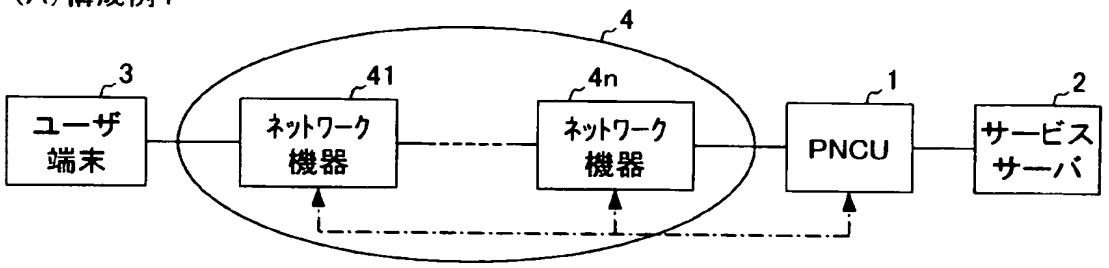
１１０　外部機器制御部

１１１　アクセスリスト

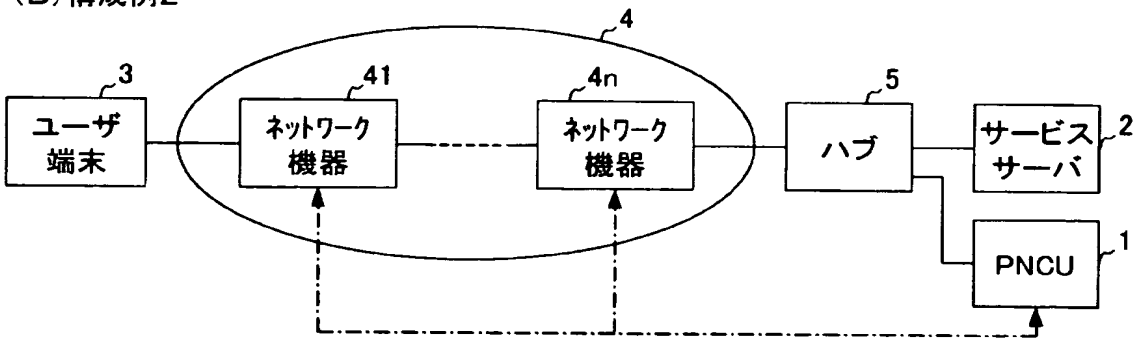
【書類名】　図面

【図１】

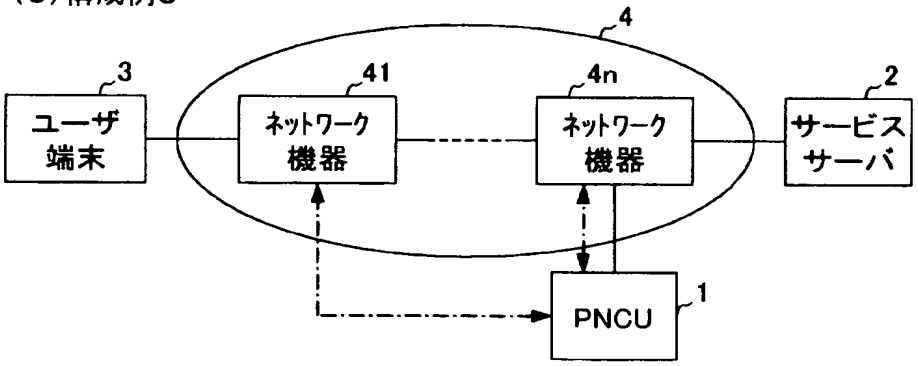
（A）構成例1



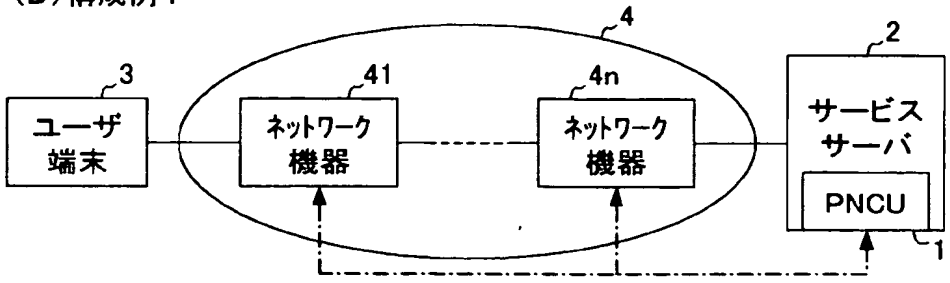
（B）構成例2



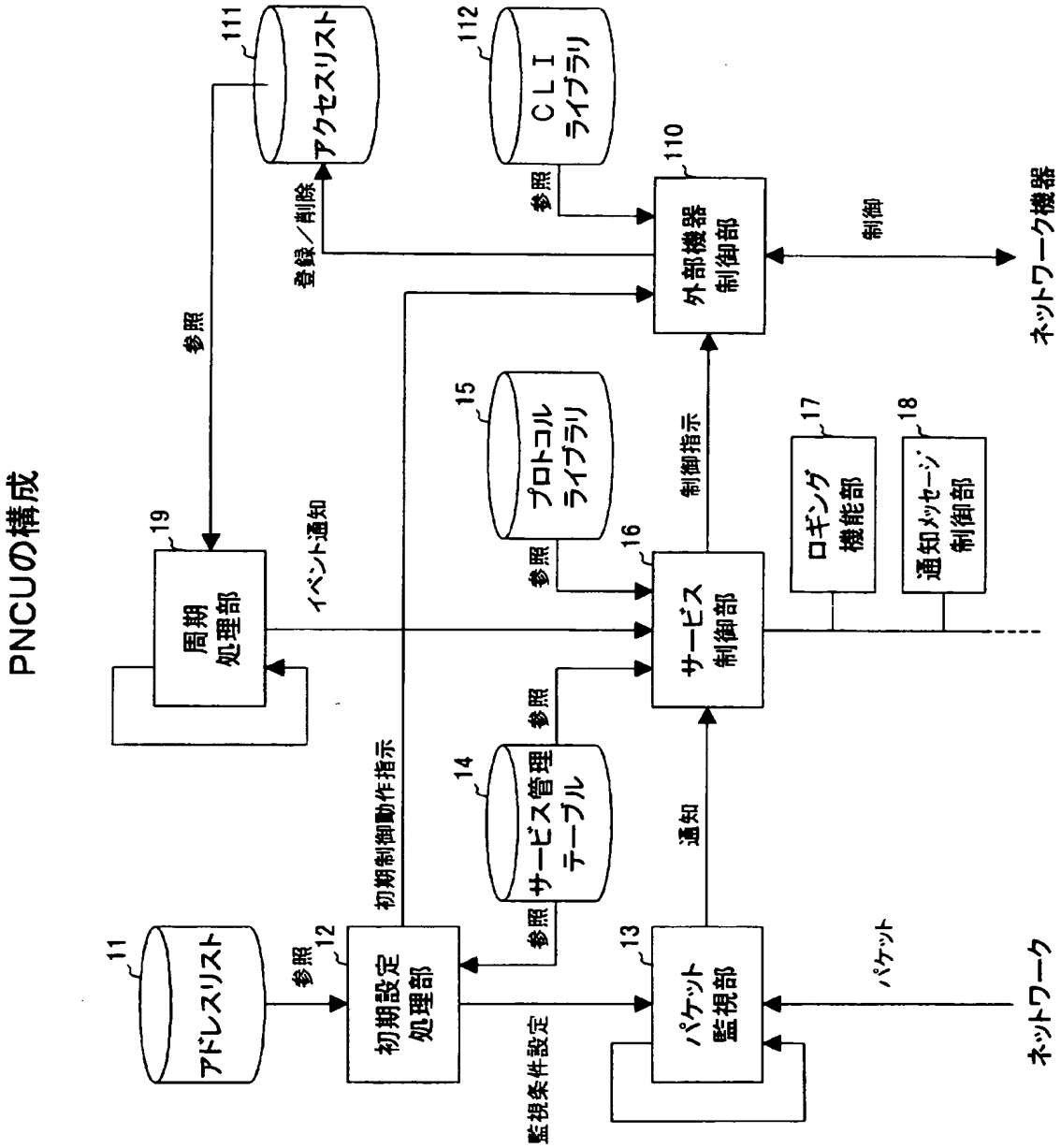
（C）構成例3



（D）構成例4

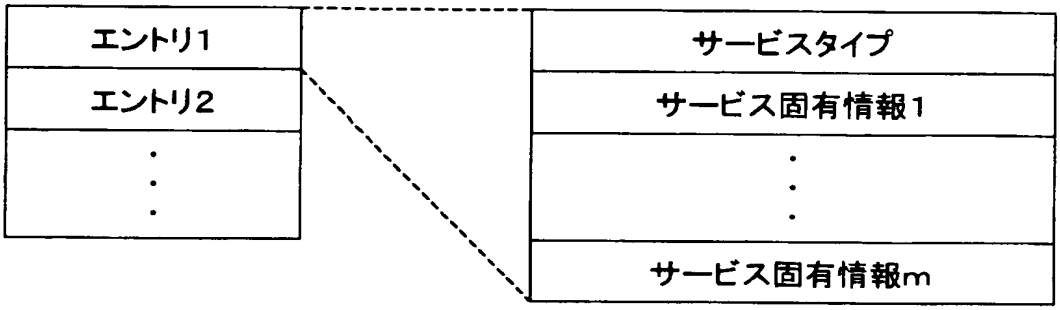


【図２】


PNCUの構成
111
アクセスリスト
112
CLI
ライブラリ
110
外部機器
制御部
ネットワーク機器
制御
登録／削除
参照
15
プロトコル
ライブラリ
17
ロギング
機能部
18
通知ﾒｯｾｰｼﾞ
制御部
制御指示
19
周期
処理部
イベント通知
16
サービス
制御部
初期制御動作指示
参照
14
サービス管理
テーブル
通知
11
アドレスリスト
12
初期設定
処理部
13
パケット
監視部
パケット
ネットワーク
監視条件設定

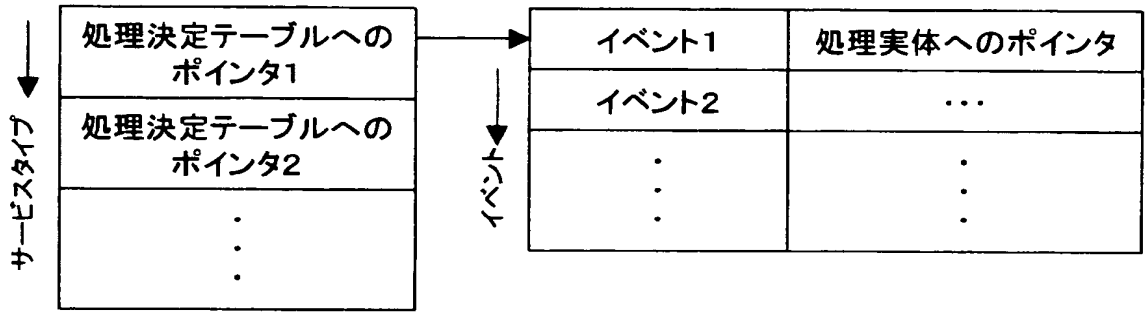
【図３】

アドレスリスト



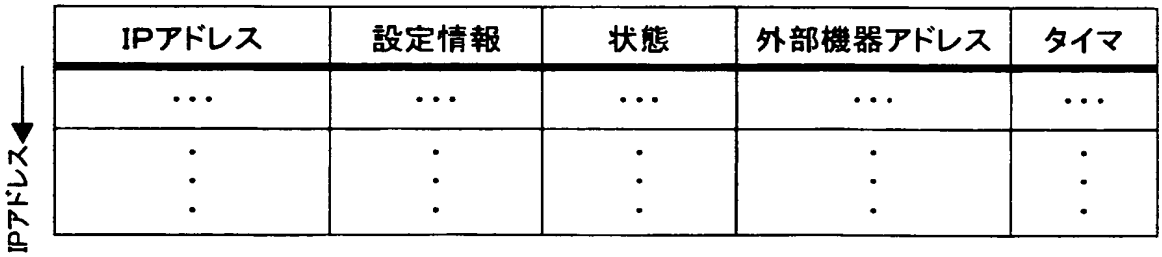
【図４】

サービス管理テーブル

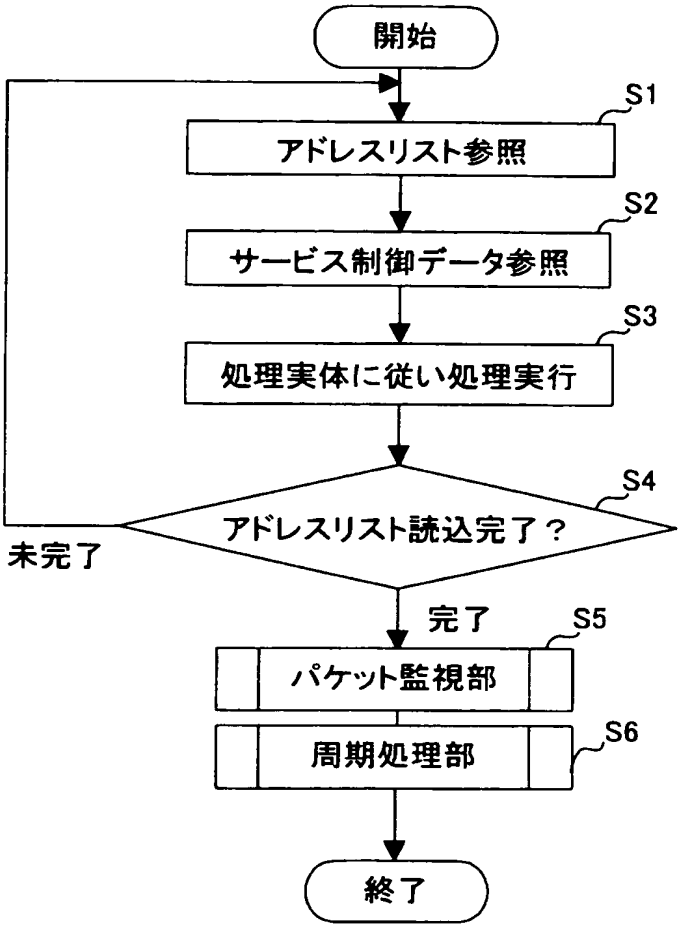


【図５】

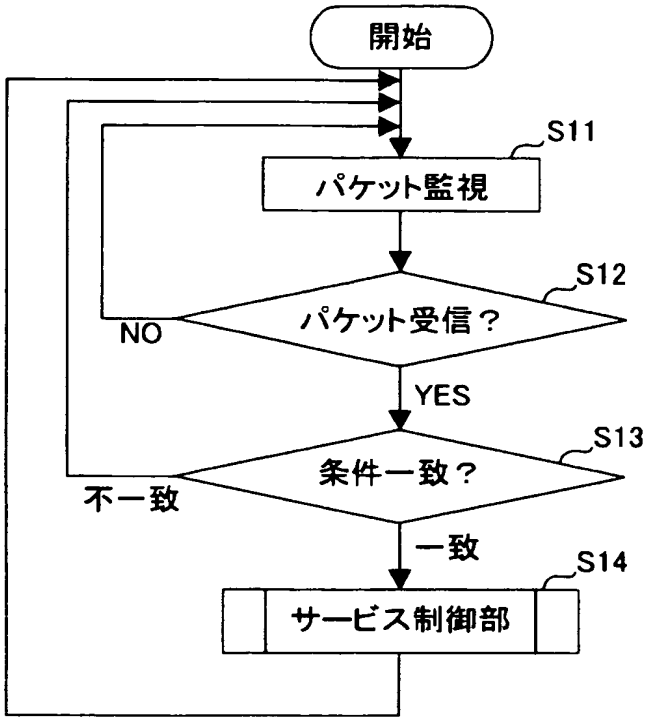
アクセスリスト



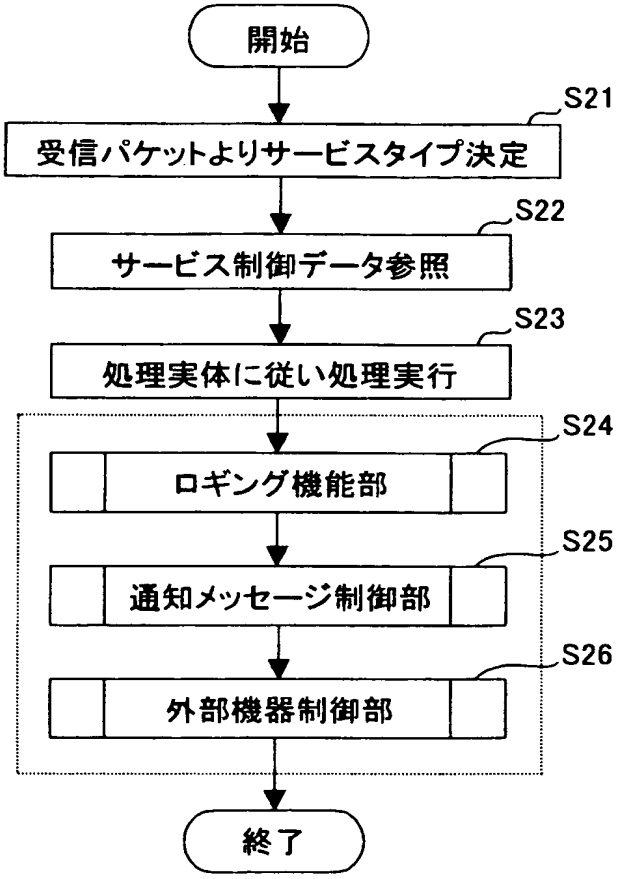
【図６】


開始
S1
アドレスリスト参照
S2
サービス制御データ参照
S3
処理実体に従い処理実行
S4
アドレスリスト読込完了？
未完了
完了
S5
パケット監視部
S6
周期処理部
終了

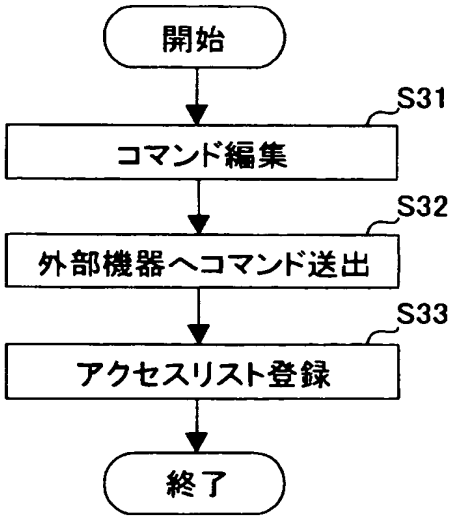
【図７】



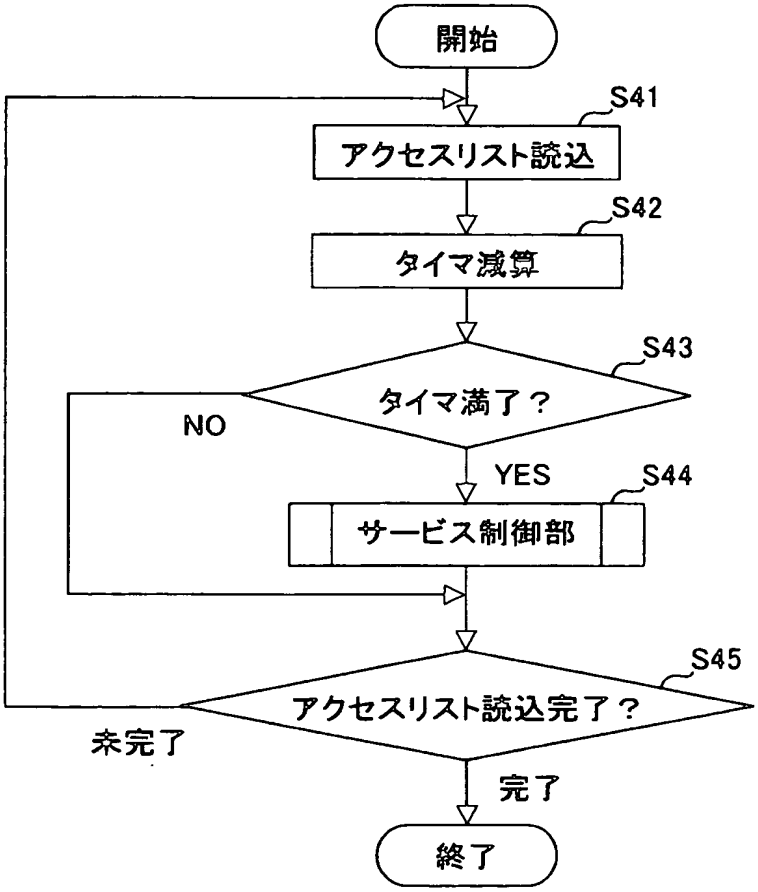
【図８】


開始
S21
受信パケットよりサービスタイプ決定
S22
サービス制御データ参照
S23
処理実体に従い処理実行
S24
ロギング機能部
S25
通知メッセージ制御部
S26
外部機器制御部
終了

【図９】

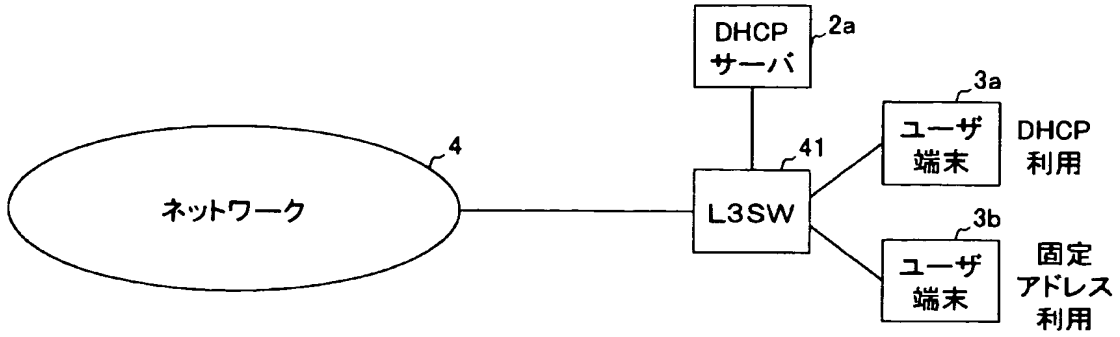

開始
S31
コマンド編集
S32
外部機器へコマンド送出
S33
アクセスリスト登録
終了

【図１０】

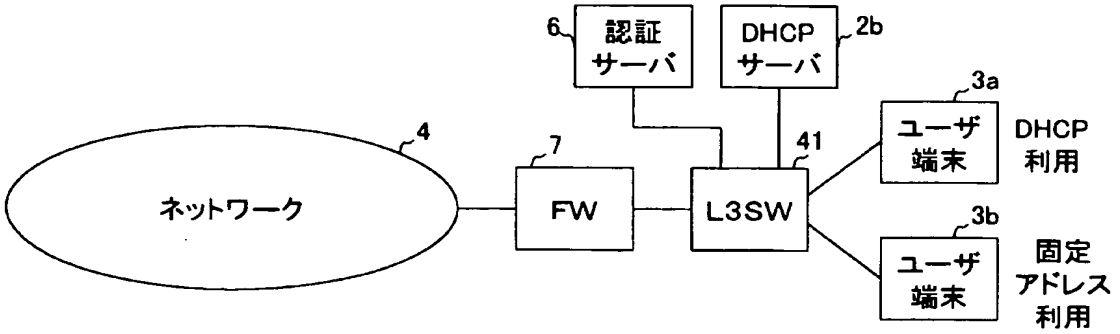

開始
S41
アクセスリスト読込
S42
タイマ減算
S43
タイマ満了？
NO
YES
S44
サービス制御部
S45
アクセスリスト読込完了？
未完了
完了
終了

【図１１】

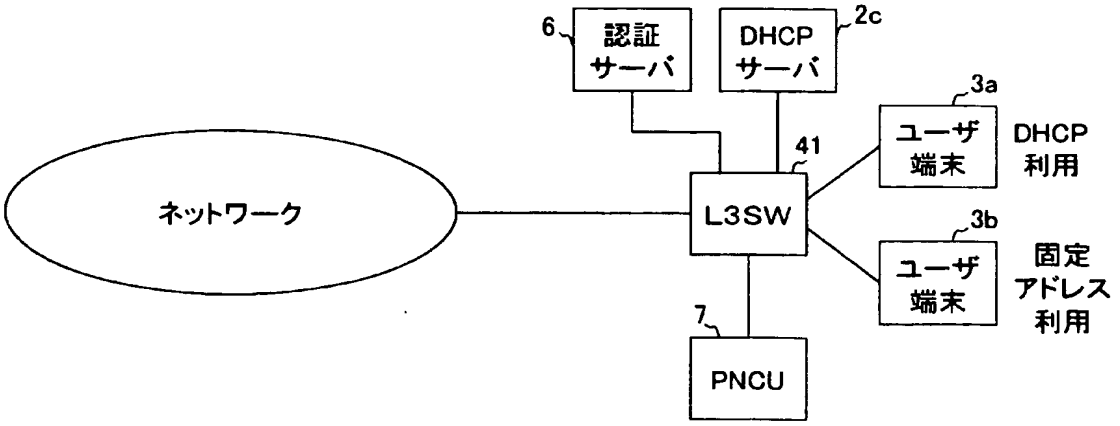
（A）DHCPのセキュリティ上の問題点



（B）従来技術による解決方法

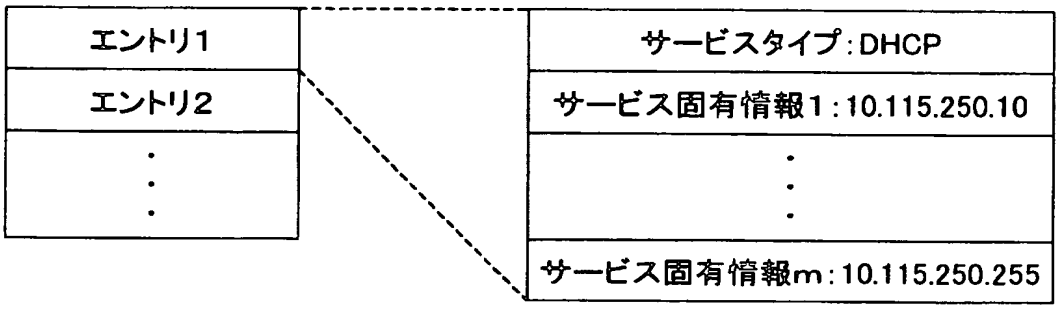


（C）本発明の実施の形態による解決方法

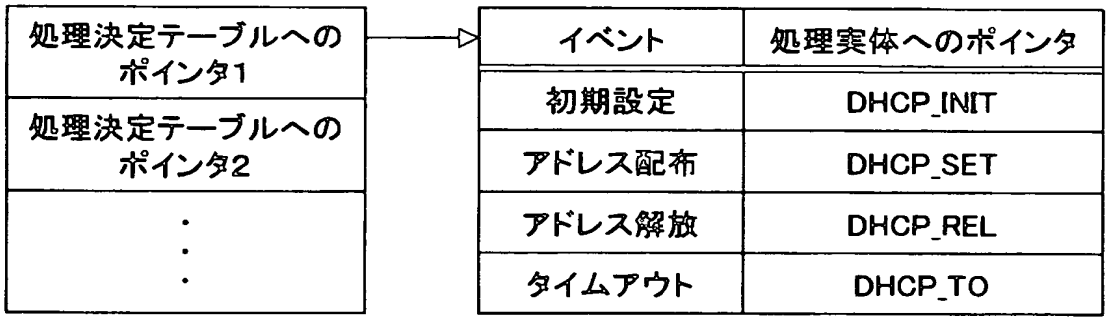


【図１２】

（A）アドレスリスト



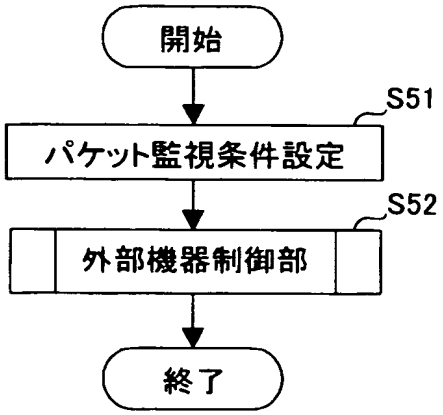
（B）サービス管理テーブル



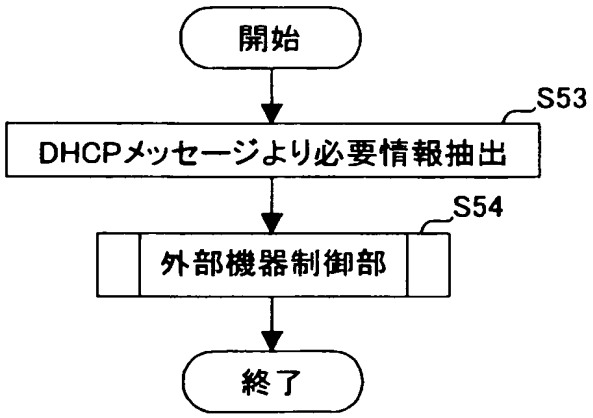
（C）アクセスリスト

IPアドレス	設定情報	状態	外部機器アドレス	タイマ
10.115.250.10	・・・	規制有り	10.115.250.1	8H
10.115.250.11	・・・	規制無し	10.115.250.1	・・・
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

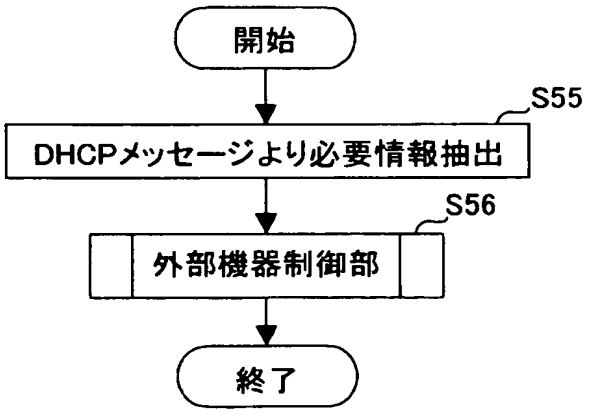
【図１３】


開始
S51
パケット監視条件設定
S52
外部機器制御部
終了

【図１４】

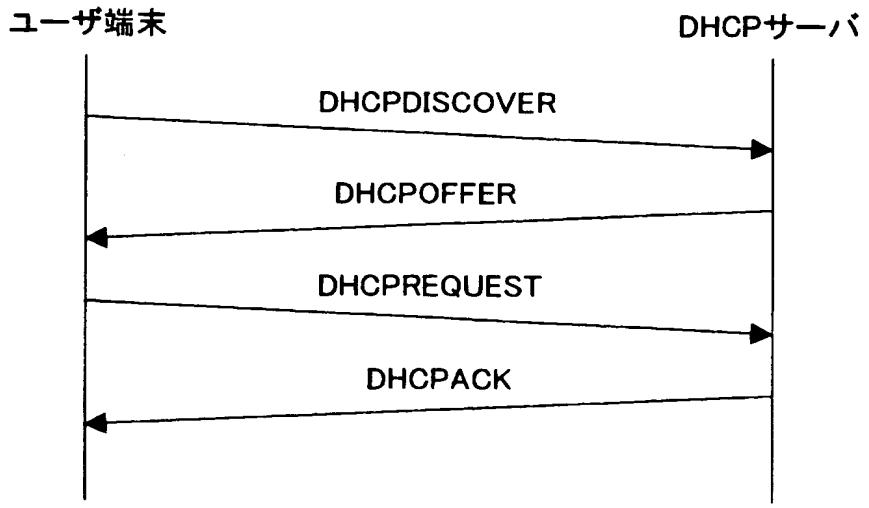

開始
S53
DHCPメッセージより必要情報抽出
S54
外部機器制御部
終了

【図１５】


開始
S55
DHCPメッセージより必要情報抽出
S56
外部機器制御部
終了

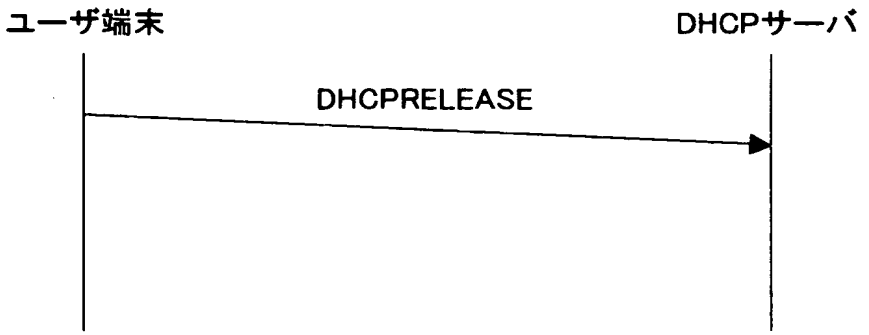
【図１６】

DHCPサーバのアドレス配布シーケンス



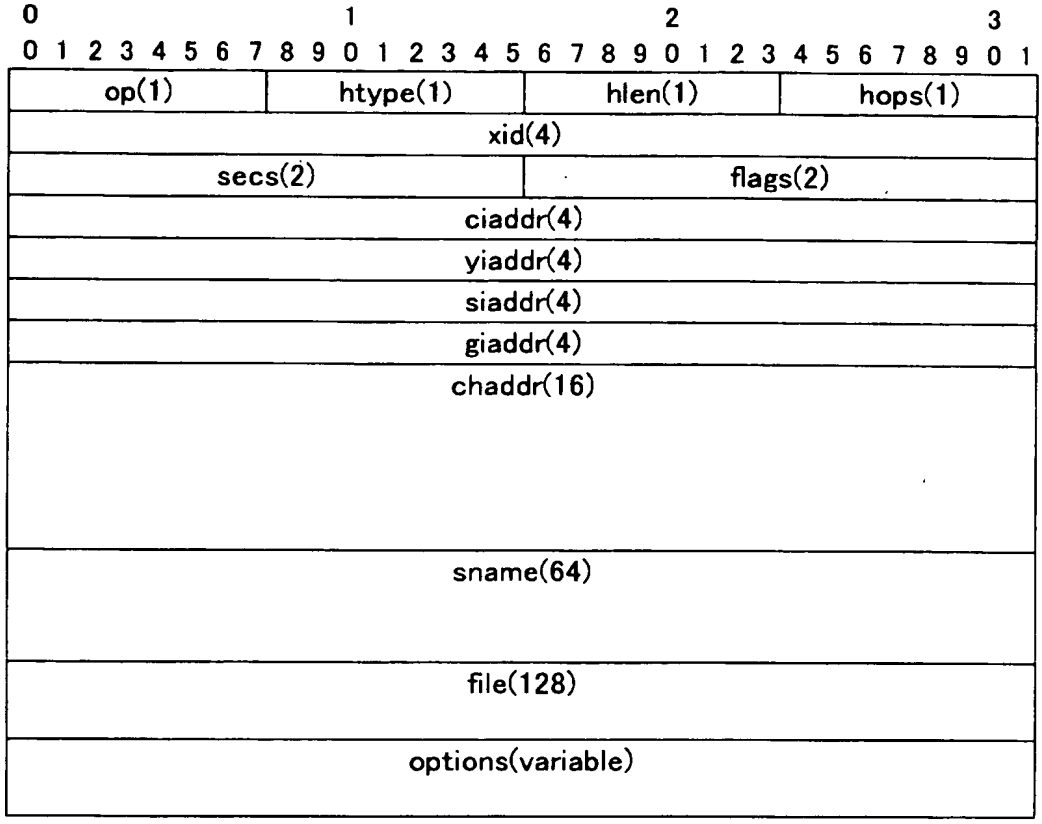
【図１７】

DHCPサーバのアドレス解放シーケンス



【図１８】

(A)DHCPメッセージフォーマット



(B)IP Address Lease Timeオプション

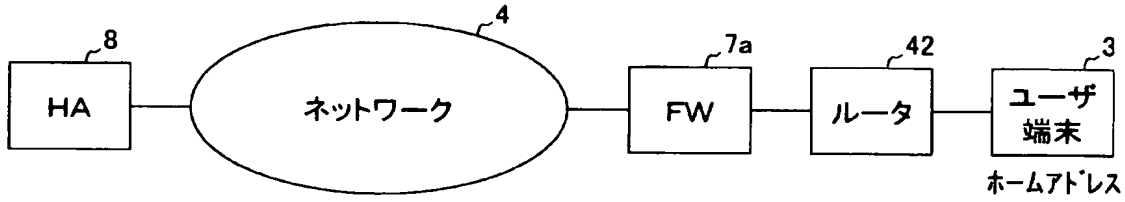
Code	Len	Lease Time			
51	4	t1	t2	t3	t4

(C)DHCP Message Typeオプション

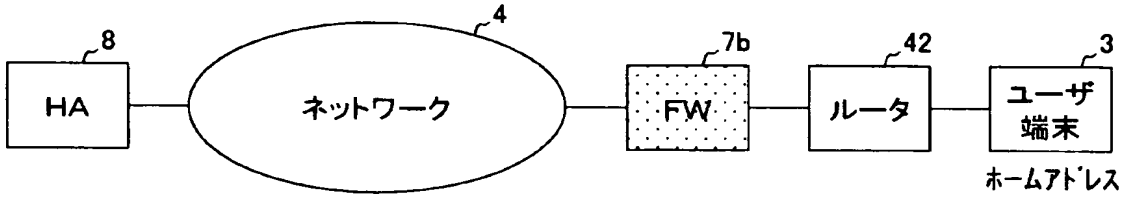
Code	Len	Type
53	1	1－9

【図１９】

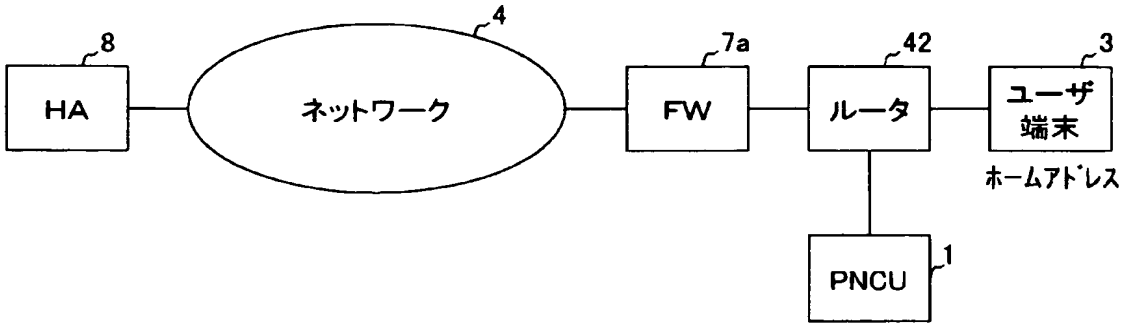
（A）Mobile IPv4のファイアウォール通過問題



（B）従来技術による解決方法

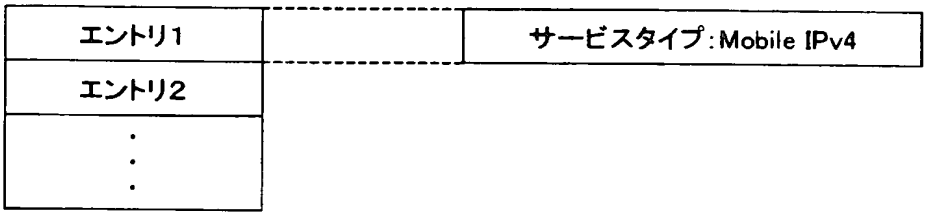


（C）本発明の実施の形態による解決方法

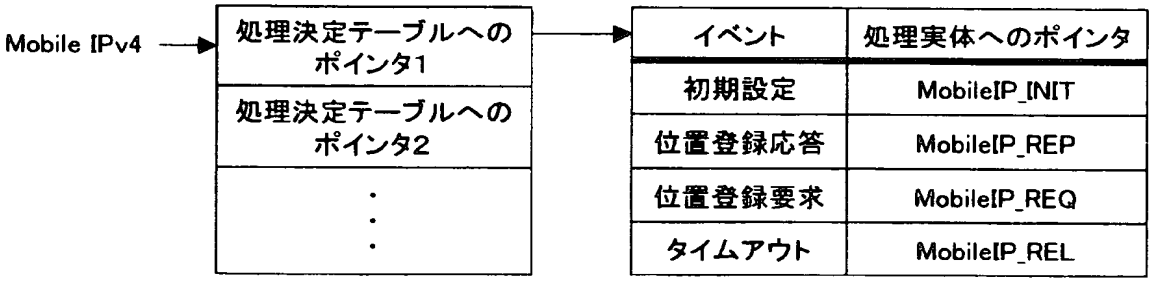


【図２０】

（A）アドレスリスト



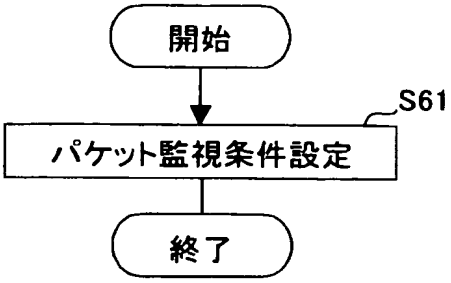
（B）サービス管理テーブル



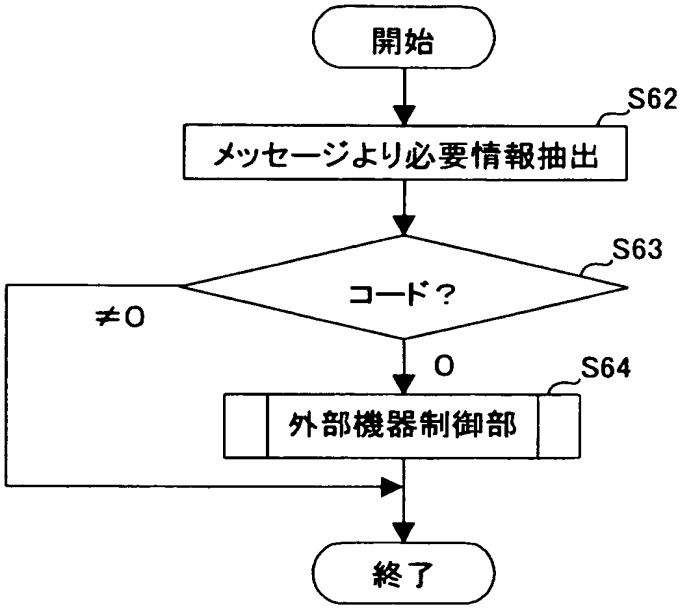
（C）アクセスリスト

IPアドレス	設定情報	状態	外部機器アドレス	タイマ
10.115.10.10	・・・	規制無し	10.115.250.1	8H
・	・	・	・	・
・	・	・	・	・
・	・	・	・	・

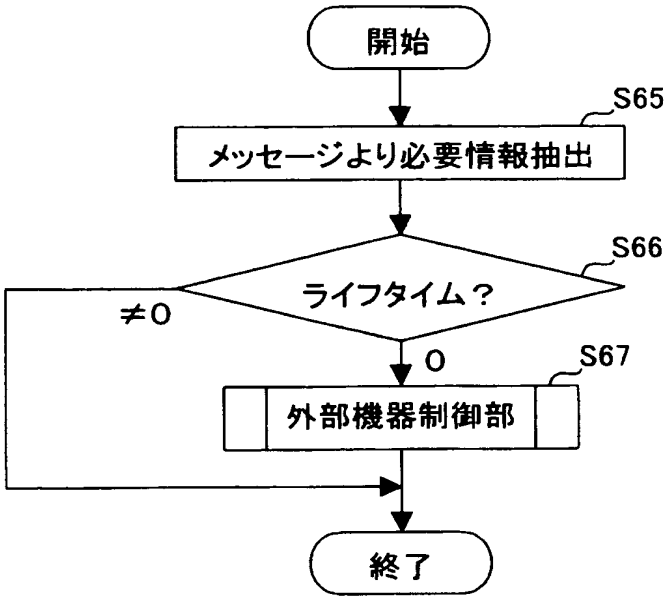
【図２１】


開始
S61
パケット監視条件設定
終了

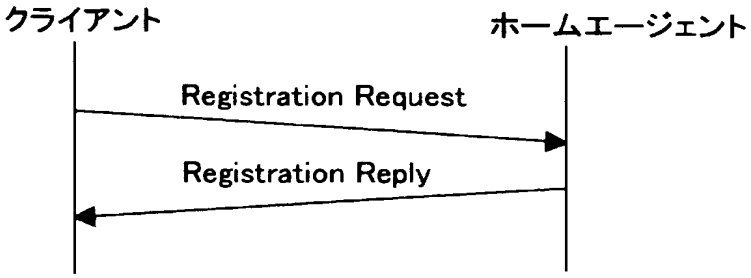
【図２２】


開始
S62
メッセージより必要情報抽出
S63
コード？
≠0
0
S64
外部機器制御部
終了

【図２３】

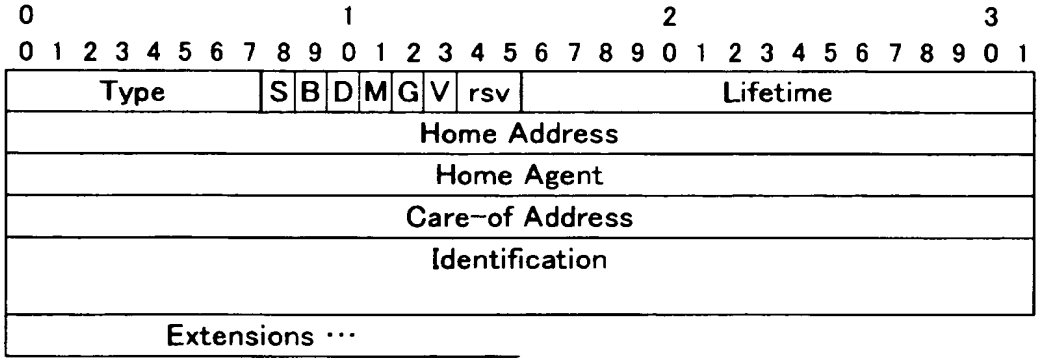

開始
S65
メッセージより必要情報抽出
S66
ライフタイム？
≠0
0
S67
外部機器制御部
終了

【図２４】

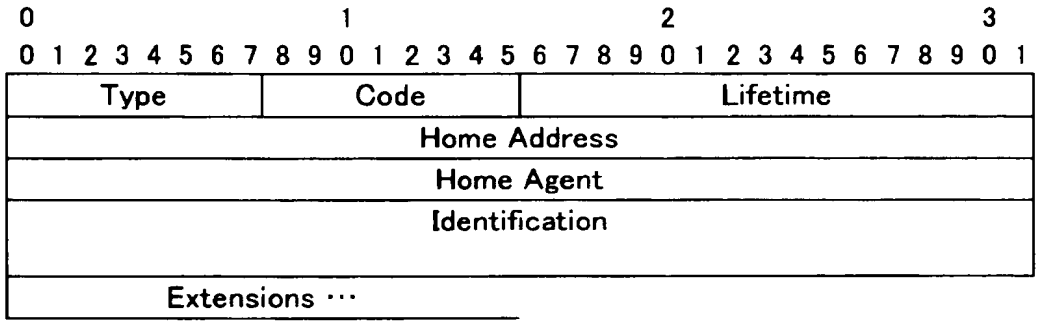

クライアント
ホームエージェント
Registration Request
Registration Reply

【図２５】

(A) Registration Request

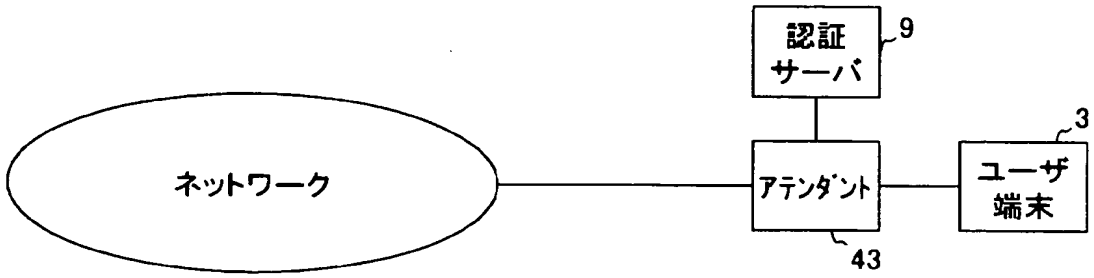


(B) Registration Reply

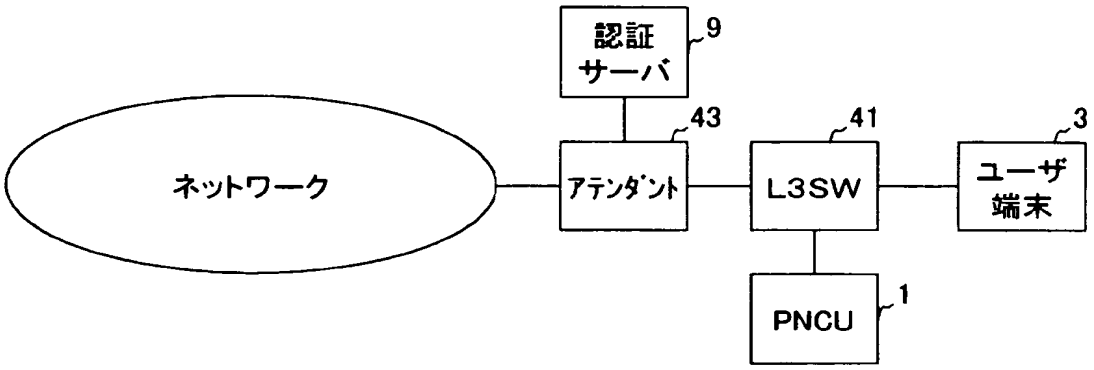


【図２６】

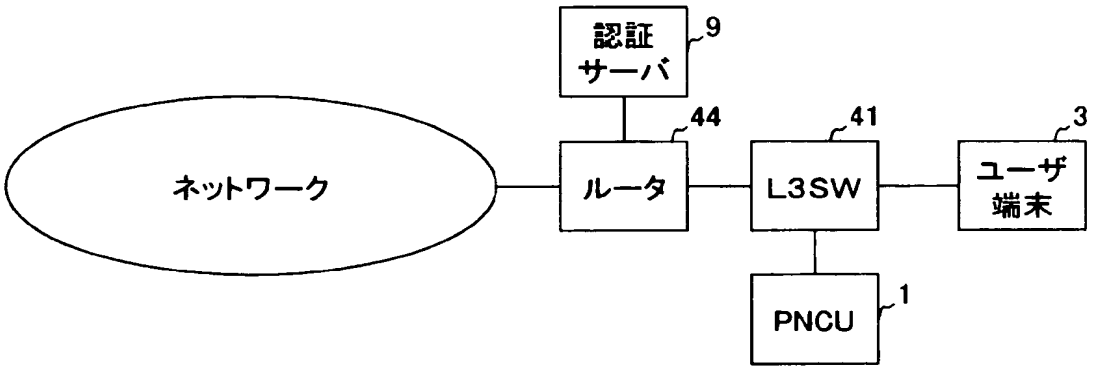
（A）IPv6におけるアクセス自動割当時のアクセス制御



（B）本発明の実施の形態による解決方法１

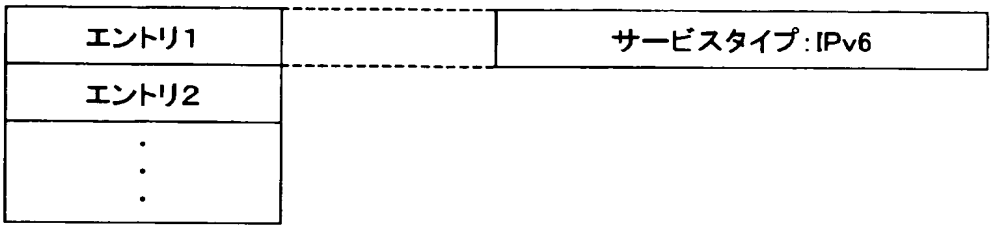


（C）本発明の実施の形態による解決方法２

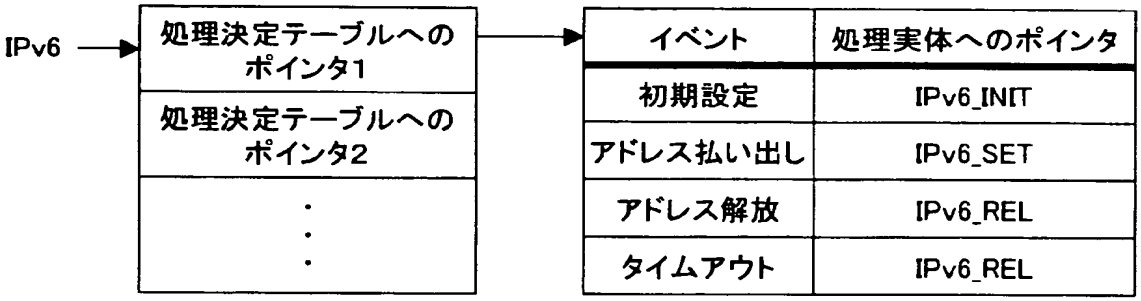


【図２７】

(A)アドレスリスト



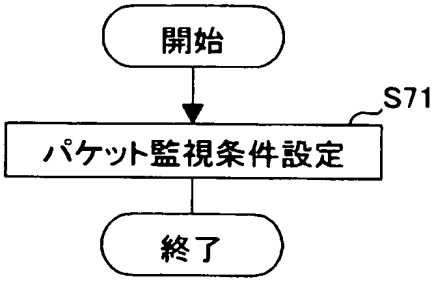
(B)サービス管理テーブル



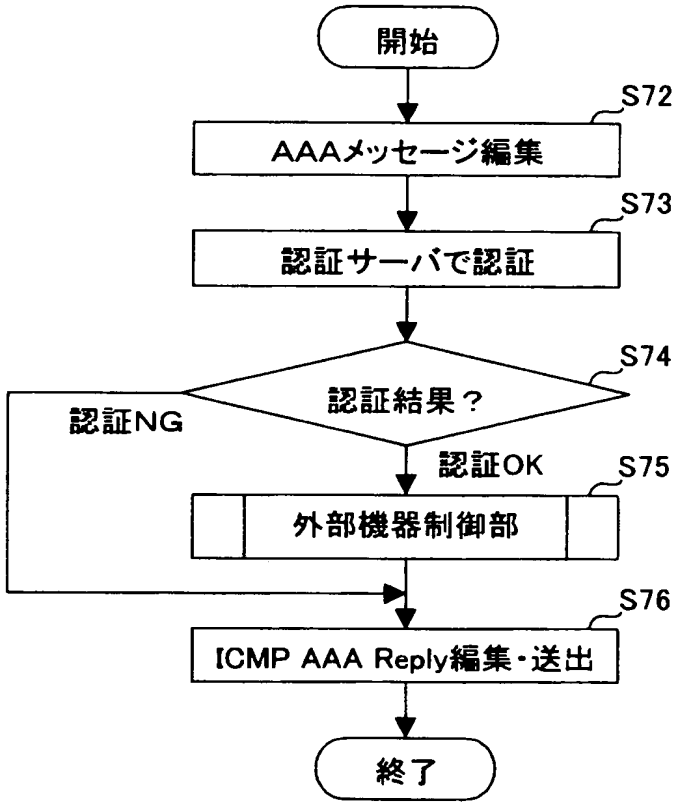
(C)アクセスリスト

IPアドレス	設定情報	状態	外部機器アドレス	タイマ
2000:10::250:56ff:fe15:100	・・・	規制無し	2000:10::250:56ff:fe15:10	8H
2000:10::250:56ff:fe15:101	・・・	規制有り	2000:10::250:56ff:fe15:10	・・・
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

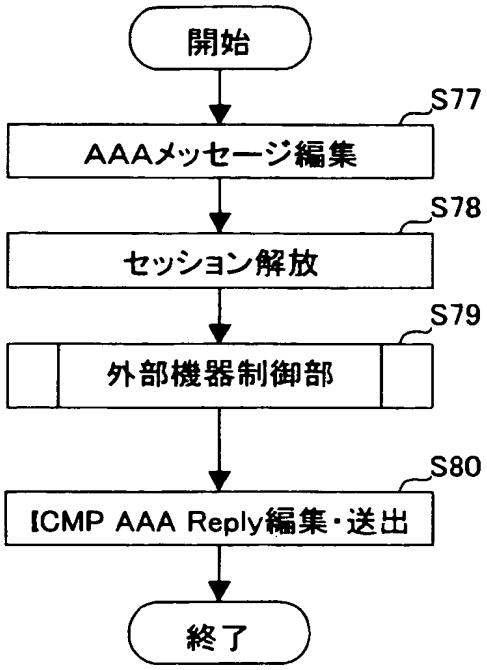
【図２８】


開始
S71
パケット監視条件設定
終了

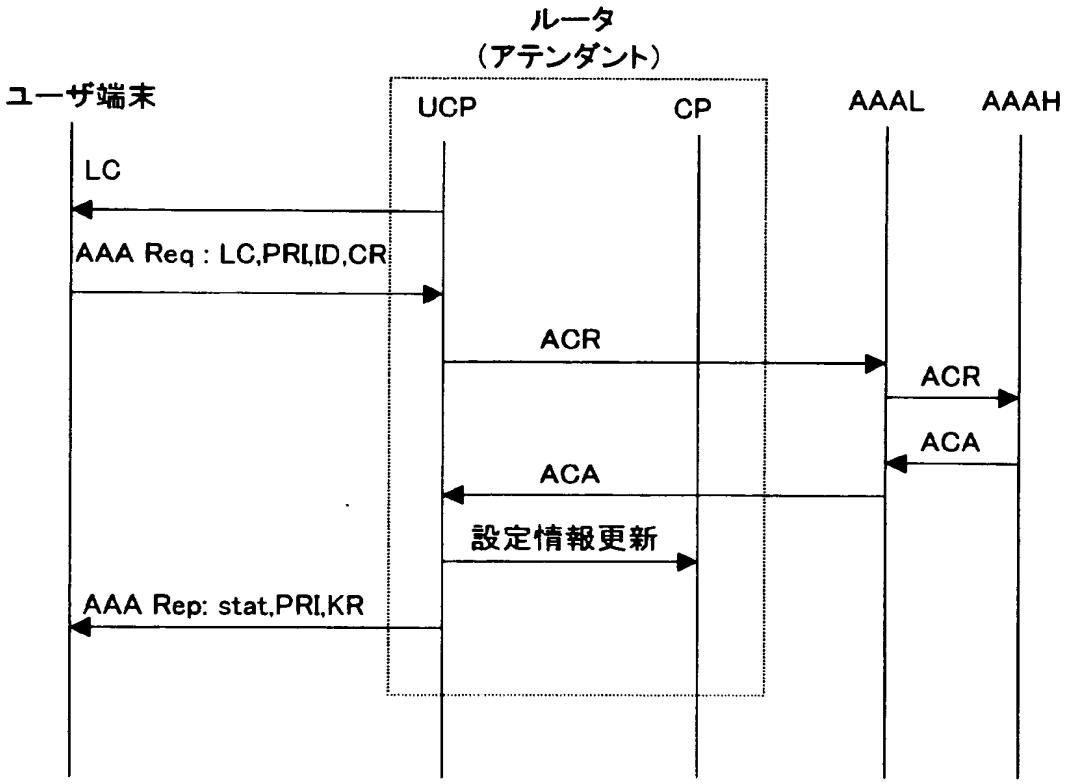
【図２９】


開始
S72
AAAメッセージ編集
S73
認証サーバで認証
S74
認証結果？
認証NG
認証OK
S75
外部機器制御部
S76
ICMP AAA Reply編集・送出
終了

【図３０】


開始
S77
AAAメッセージ編集
S78
セッション解放
S79
外部機器制御部
S80
ICMP AAA Reply編集・送出
終了

【図３１】



LC = ローカル AAA チャレンジ

RPI = ホストと AAAH 間で用いられる再送保護指標

CR = AAA 証明書

ID = クライアント識別子

KR = 鍵応答

UCP = 非制御部分

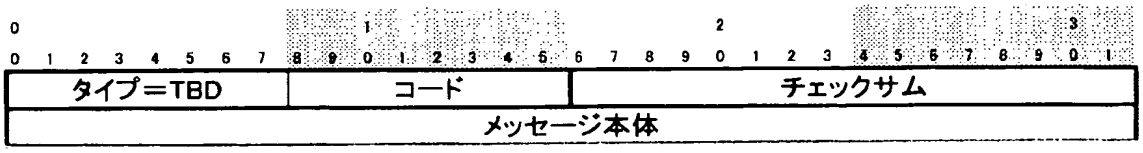
CP = 制御部分

ACR = AAA クライアント要求（AAA プロトコル使用）

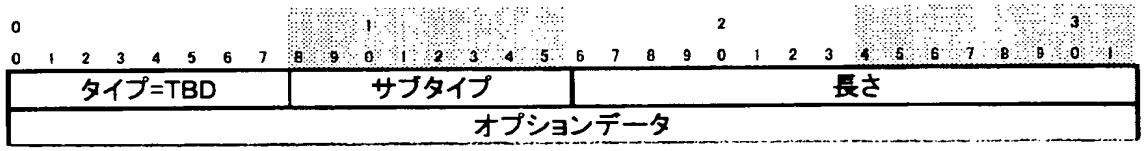
ACA = AAA クライアント応答（AAA プロトコル応答）

【図３２】

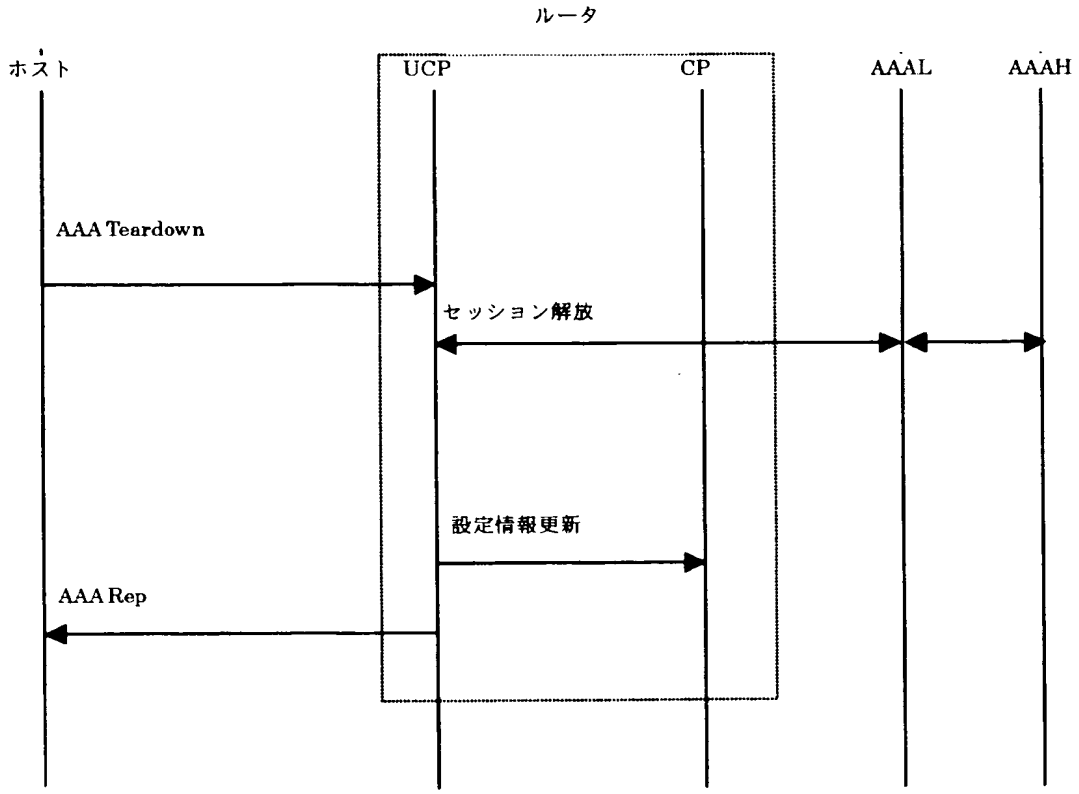
（１）ＩＣＭＰ　ＡＡＡメッセージ



（２）ＡＡＡプロトコルオプション



【図３３】



【書類名】　　要約書

【要約】

【課題】　ネットワークの既存の装置やネットワークの構成に変更を加えることなく，ネットワークの機能を補完または拡張する。

【解決手段】　ユーザ端末３と，ユーザ端末３に所定のサービスを提供するサービスサーバ２との間で通信されるパケットを監視できる位置に，代理ネットワーク制御装置（ＰＮＣＵ）１が配置される。ＰＮＣＵ１は，ユーザ端末３とサービスサーバ２との間で通信されるパケットを監視し，該パケットに基づいて，ネットワーク機器４１～４ｎの少なくとも１つを制御することにより，サービスサーバ２の機能を補完または拡張する機能を実行する。たとえば，サービスサーバ２がＤＨＣＰサーバである場合には，ＰＮＣＵ１は，ＤＨＣＰサーバからユーザ端末３に発行されたＩＰアドレスを送信元アドレスとして有するパケットのみが転送されるようにネットワーク機器を制御する。

【選択図】　　図１

特願２００２－３４６９４９

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　新規登録
住　所　神奈川県川崎市中原区上小田中１０１５番地
氏　名　富士通株式会社

２．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社